TRIANGULAR BASES OF INTEGRAL CLOSURES

HAYDEN D. STAINSBY

Abstract. In this work, we consider the problem of computing triangular bases of integral closures of one-dimensional local rings.

Let (K, v) be a discrete valued field with valuation ring $\mathcal{O}$ and let $\mathfrak{m}$ be the maximal ideal. We take $f \in \mathcal{O}[x]$, a monic irreducible polynomial of degree n and consider the extension $L = K[x]/(f(x))$ as well as $\mathcal{O}_L$ the integral closure of $\mathcal{O}$ in L, which we suppose to be finitely generated as an $\mathcal{O}$-module.

The algorithm MaxMin, presented in this paper, computes triangular bases of fractional ideals of $\mathcal{O}_L$. The theoretical complexity is equivalent to current state of the art methods and in practice is almost always faster. It is also considerably faster than the routines found in standard computer algebra systems, excepting some cases involving very small field extensions.

1. Introduction

Let (K, v) be a discrete valued field with valuation ring $\mathcal{O}$. Let $\mathfrak{m}$ be the maximal ideal, $\pi \in \mathfrak{m}$ a generator of $\mathfrak{m}$ and $\mathbb{F} = \mathcal{O}/\mathfrak{m}$ the residue class field.

Let K_v be the completion of K, and retain $v : \overline{K}_v^* \to \mathbb{Q}$ the canonical extension of v to a fixed algebraic closure of K_v. Let $\mathcal{O}_v$ be the valuation ring of K_v.

Let $f \in \mathcal{O}[x]$ be a monic, irreducible polynomial of degree n and fix a root $\theta \in \overline{K}$ in an algebraic closure of K. Let $L = K(\theta)$ be the corresponding finite extension of K and let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}$ in L, which is a Dedekind domain. We denote the set of non-zero prime ideals of $\mathcal{O}_L$ by $\mathcal{P}$.

We suppose that $\mathcal{O}_L$ is finitely generated as an $\mathcal{O}$-module. This condition holds under very natural assumptions; for instance, if L/K is separable, or (K, v) is complete, or $\mathcal{O}$ is a finitely generated algebra over a field [12, Ch.I, §4]. Under this hypothesis, $\mathcal{O}_L$ is a free $\mathcal{O}$-module of rank n. An $\mathcal{O}$-basis of $\mathcal{O}_L$ is called a *v-integral basis* of $\mathcal{O}_L$.

The computation of v-integral bases is an essential task in computational arithmetic geometry. We are interested in constructing *reduced triangular* v-integral bases. Let us clarify these concepts.

Definition 1.1. *For each prime ideal $\mathfrak{p} \in \mathcal{P}$, we consider the normalised valuation:*

$$w_{\mathfrak{p}} := e(\mathfrak{p}/\mathfrak{m})^{-1} v_{\mathfrak{p}} \colon L \longrightarrow e(\mathfrak{p}/\mathfrak{m})^{-1}\mathbb{Z} \cup \{\infty\},$$

where $v_{\mathfrak{p}}$ is the canonical discrete valuation of L attached to $\mathfrak{p}$ and $e(\mathfrak{p}/\mathfrak{m})$ is the ramification index. Also, we define

$$w \colon L \longrightarrow \mathbb{Q} \cup \{\infty\}, \quad \alpha \mapsto \operatorname{Min}\{w_{\mathfrak{p}}(\alpha) \colon \mathfrak{p} \in \mathcal{P}\}.$$

2010 *Mathematics Subject Classification.* Primary 11Y40; Secondary 11R04, 14H05, 13P05.

Key words and phrases. fractional ideal, local field, Montes algorithm, Newton polygon, integral basis, OM representation, type, discrete valuation.

Partially supported by MTM2013-40680-P from the Spanish MEC.

Clearly, an element $\alpha \in L$ belongs to $\mathcal{O}_L$ if and only if $w(\alpha) \geqslant 0$.

Definition 1.2. *A triangular family of elements in $\mathcal{O}_L$, are elements*

$$\frac{g_0(\theta)}{\pi^{k_0}}, \frac{g_1(\theta)}{\pi^{k_1}}, \ldots, \frac{g_{n-1}(\theta)}{\pi^{k_{n-1}}},$$

such that for all $0 \leqslant i < n$ the polynomial $g_i(x) \in \mathcal{O}[x]$ is monic of degree i, and k_i is a non-negative integer such that $k_i \leqslant w\left(g_i(\theta)\right)$.

A triangular basis of $\mathcal{O}_L$ is a triangular family which is a v-integral basis.

Definition 1.3. *A family $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$ is called reduced if for any family $a_1, \ldots, a_n \in \mathcal{O}$:*

$$w\left(\sum_{i=1}^{n} a_i\alpha_i\right) = \operatorname{Min}\left\{w(a_i\alpha_i) : 1 \leqslant i \leqslant n\right\}.$$

There are well-known conditions on a triangular family characterising when it is a reduced basis.

Theorem 1.4. *Let $\mathcal{B} = \left(g_0(\theta)/\pi^{\lfloor \nu_0 \rfloor}, \ldots, g_{n-1}(\theta)/\pi^{\lfloor \nu_{n-1} \rfloor}\right)$ be a triangular family in $\mathcal{O}_L$ with $\nu_i = w(g_i(\theta))$ for all $0 \leqslant i < n$. Then,*

1. *$\mathcal{B}$ is a triangular basis if and only if $\lfloor \nu_i \rfloor \geqslant \lfloor w\left(h(\theta)\right) \rfloor$ for all $h \in \mathcal{O}[x]$ monic of degree i and all $0 \leqslant i < n$.*
2. *$\mathcal{B}$ is a reduced triangular basis if and only if $\nu_i \geqslant w\left(h(\theta)\right)$ for all $h \in \mathcal{O}[x]$ monic of degree i and all $0 \leqslant i < n$.*

Therefore, to construct a reduced triangular $\mathcal{O}$-basis of $\mathcal{O}_L$ it suffices to find for each $0 \leqslant i < n$ a polynomial $g_i \in \mathcal{O}[x]$ monic of degree i such that $w\left(g_i(\theta)\right)$ is maximal amongst all monic polynomials in $\mathcal{O}[x]$ of the same degree.

The aim of the paper is to present the *MaxMin algorithm*, a very simple procedure to construct these optimal polynomials g_i.

The desire to compute triangular local bases comes from their utility in constructing global bases. Let A be a PID and let B be the integral closure of A in a finite extension of its field of fractions. If B is free as an A-module, then an A-basis of B can be computed by patching local integral bases of $B_{\mathfrak{m}}$ as an $A_{\mathfrak{m}}$-module for an adequate finite set of non-zero prime ideals $\mathfrak{m} \in \operatorname{Spec}(A)$.

This patching process, usually based on the Chinese remainder theorem, is efficient only if the local bases are triangular. In this case, the global A-basis of B one obtains is triangular too.

The property of *reducedness* is important for certain applications in function fields [1]. The MaxMin algorithm has the advantage of producing local bases which are also reduced.

MaxMin is an OM algorithm, it works with data derived from an *OM factorisation* of the polynomial f in $\mathcal{O}_v[x]$. In 1999, J. Montes extended some ideas of Ore and MacLane and implemented an algorithm to compute a representation of the prime ideals of $\mathcal{O}_L$ by way of factoring the defining polynomial f over $\mathcal{O}_v[x]$. This "Montes algorithm" coupled with work by K. Okutsu on constructing explicit integral bases of local fields, gave rise to several theoretical developments concerning *OM representations* of prime ideals [3, 4, 5, 6, 8, 9, 11].

There are other methods for the computation of integral bases based on a previous computation of an OM factorisation of the defining polynomial f. In [6, Sec.

6] a method was presented based in the computation of certain *multipliers*, following an old idea of Ore. In [7] a more direct *method of the quotients* was presented, which obtains the numerators of a reduced basis by multiplying certain polynomials obtained as a by-product of the OM factorisation algorithm.

These OM methods are extremely fast in practice and their theoretical complexity is lower than that of the traditional methods based mainly on the Round-2 and Round-4 routines by Zassenhaus and Ford. However, both OM methods yield non-triangular bases, and so a triangularisation routine must be applied to the local bases before they can be used to construct a global basis. These linear procedures are slow in practice and constitute a bottleneck for the whole process.

The MaxMin algorithm yields reduced triangular local bases by a direct method, which avoids the use of linear techniques. This makes MaxMin much more efficient in practice. Another advantage of MaxMin is that the method is equally valid for the computation of bases of fractional ideals. This is particularly useful for the computation of bases of Riemann-Roch spaces of divisors of algebraic curves, which requires the computation of bases of certain fractional ideals attached to the divisor.

It is common in many computational algebra systems, to provide bases in Hermite Normal Form (HNF). This serves two purposes, the first is that canonical bases simplify the comparison of the rings that they generate. The second is that bases in HNF are triangular, and so patching of global bases from local bases is more efficient. However, the routines used to compute the HNF of a given basis require considerably more time than the computation of a basis.

By using the MaxMin algorithm we can offer two distinct improvements. By computing a triangular basis directly, in many circumstances, we do not need HNF at all, resulting in a significant improvement in execution time. Secondly, if HNF is indeed required, it is faster to compute the HNF of a basis which is already triangular, compared to a random basis.

We review OM representations of prime ideals in Section 2. In Section 3 the algorithm MaxMin will be introduced. In Section 4 we will discuss some computational examples. Finally, the proofs of the two main theorems from Sections 2 and 3 will be deferred until Sections 5 and 6.

2. OM representations of prime ideals

The prime ideals of $\mathcal{O}_L$ are in 1-to-1 correspondence with the prime factors of f in $\mathcal{O}_v[x]$. Let $f = \prod_{\mathfrak{p}\in\mathcal{P}} F_{\mathfrak{p}}$ be the factorisation of f into a product of monic irreducible polynomials $F_{\mathfrak{p}} \in \mathcal{O}_v[x]$. Let $n_{\mathfrak{p}} = \deg F_{\mathfrak{p}} = e(\mathfrak{p}/\mathfrak{m})f(\mathfrak{p}/\mathfrak{m})$.

Inspired by ideas of Ore and MacLane, J. Montes developed an algorithm to compute *OM representations*

$$\mathbb{t}_{\mathfrak{p}} = \left(\psi_{0,\mathfrak{p}}; (\phi_{1,\mathfrak{p}}, \lambda_{1,\mathfrak{p}}, \psi_{1,\mathfrak{p}}); \ldots; (\phi_{r_{\mathfrak{p}},\mathfrak{p}}, \lambda_{r_{\mathfrak{p}},\mathfrak{p}}, \psi_{r_{\mathfrak{p}},\mathfrak{p}}); (\phi_{\mathfrak{p}}, \lambda_{\mathfrak{p}}, \psi_{\mathfrak{p}})\right), \tag{1}$$

of each prime factor $F_{\mathfrak{p}}$. An object $\mathbb{t}_{\mathfrak{p}}$ as in (1) is a *type*; it contains several data structured into levels, encoding relevant arithmetic information about the polynomial $F_{\mathfrak{p}}$ and the prime ideal $\mathfrak{p}$. For the precise definition of a type, we refer to [8]. We now recall some of the properties of the invariants of a type.

The number $r_{\mathfrak{p}} + 1$ of levels is called the *order* of the type and $r_{\mathfrak{p}}$ is the *Okutsu depth* of $F_{\mathfrak{p}}$. The family of polynomials $[\phi_{1,\mathfrak{p}}, \ldots, \phi_{r_{\mathfrak{p}},\mathfrak{p}}]$ is an *Okutsu frame* of $F_{\mathfrak{p}}$. These are monic polynomials in $\mathcal{O}[x]$ which are irreducible in $\mathcal{O}_v[x]$.

If we denote $m_i = \deg \phi_{i,\mathfrak{p}}$, we have

$$m_1 \mid \cdots \mid m_{r_\mathfrak{p}} \mid m_{r_\mathfrak{p}+1} = n_\mathfrak{p}, \qquad m_1 < \cdots < m_{r_\mathfrak{p}} < m_{r_\mathfrak{p}+1} = n_\mathfrak{p}. \tag{2}$$

The polynomial $\phi_{r_\mathfrak{p}+1,\mathfrak{p}} := \phi_\mathfrak{p}$ is an *Okutsu approximation* to $F_\mathfrak{p}$; it is a monic polynomial in $\mathcal{O}[x]$ of degree $n_\mathfrak{p}$ which is "sufficiently close" to $F_\mathfrak{p}$ for many purposes. More precisely,

$$v\left(\phi_\mathfrak{p}(\theta)\right) > \frac{n_\mathfrak{p}}{m_{r_\mathfrak{p}}} v\left(\phi_{r_\mathfrak{p},\mathfrak{p}}(\theta)\right).$$

The data $\lambda_{i,\mathfrak{p}}, \lambda_\mathfrak{p}$ are positive rational numbers called the *slopes* of the type. Typically, one denotes $\lambda_{i,\mathfrak{p}} = h_i/e_i$, $\lambda_{r_\mathfrak{p}+1,\mathfrak{p}} := \lambda_\mathfrak{p} = h_{r_\mathfrak{p}+1}/e_{r_\mathfrak{p}+1}$ the positive (coprime) numerator and denominator of the slope. One has $e_{r_\mathfrak{p}+1} = 1$.

The type determines a chain of finite extensions of the residue field $\mathbb{F}$:

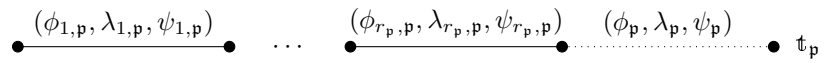
$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_{r_\mathfrak{p}+1} = \mathbb{F}_\mathfrak{p},$$

where $\mathbb{F}_\mathfrak{p}$ is isomorphic to the residue class field of the finite extension of K_v determined by $F_\mathfrak{p}$. The polynomial $\psi_{0,\mathfrak{p}} \in \mathbb{F}[y]$ is one of the prime factors of the reduction of f modulo $\mathfrak{m}$. The *residual polynomials* $\psi_{i,\mathfrak{p}} \in \mathbb{F}_i[y]$ are monic and irreducible; they determine the next extension: $\mathbb{F}_{i+1} = \mathbb{F}_i[y]/(\psi_{i,\mathfrak{p}})$, for all $0 \leqslant i \leqslant r_\mathfrak{p}$. The monic polynomial $\psi_{r_\mathfrak{p}+1,\mathfrak{p}} := \psi_\mathfrak{p} \in \mathbb{F}_\mathfrak{p}[y]$ has degree one. For $i > 0$, one has $\psi_{i,\mathfrak{p}} \neq y$.

If we denote $f_i := \deg \psi_{i,\mathfrak{p}}$, we have

$$e(\mathfrak{p}/\mathfrak{m}) = e_1 \cdots e_{r_\mathfrak{p}}, \qquad f(\mathfrak{p}/\mathfrak{m}) = f_0 \cdots f_{r_\mathfrak{p}}, \qquad m_i = e_1 f_1 \cdots e_{i-1} f_{i-1}. \tag{3}$$

We may consider each type $\mathfrak{t}_\mathfrak{p}$ as a path with root note ψ_0 where each level is written along the edges:

(4)


Each node $\mathfrak{t}$ of this path is identified with the type obtained by gathering all level data from the edges joining $\mathfrak{t}$ with the root node.

The last edge is dotted to emphasise that $e_{r_\mathfrak{p}+1} f_{r_\mathfrak{p}+1} = 1$, while for all other edges we have $e_i f_i > 1$ as (2) and (3) show.

Actually, the depth $r_\mathfrak{p}$ and the data $(\phi_{i,\mathfrak{p}}, \lambda_{i,\mathfrak{p}}, \psi_{i,\mathfrak{p}})$ of all levels $i \leqslant r_\mathfrak{p}$ are (up to certain equivalence relation) canonical data attached to $F_\mathfrak{p}$ [8, Sec. 3.3]. On the other hand, the last level $(\phi_\mathfrak{p}, \lambda_\mathfrak{p}, \psi_\mathfrak{p})$ strongly depends on the choice of $\phi_\mathfrak{p}$.

For the proof of the next result, see [8, Sec. 4].

Lemma 2.1. *Let $\phi \in \mathcal{O}[x]$ be any monic polynomial of degree $n_\mathfrak{p}$ that satisfies $v\left(\phi(\theta)\right) \geqslant v\left(\phi_\mathfrak{p}(\theta)\right)$. Then, for adequate choice of $\lambda \in \mathbb{Z}_{>0}$ and $a \in \mathbb{F}_\mathfrak{p}^*$, the object:*

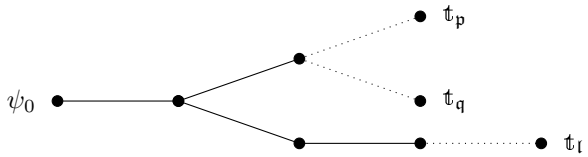
$$\mathfrak{t}'_\mathfrak{p} = \left(\psi_{0,\mathfrak{p}}; (\phi_{1,\mathfrak{p}}, \lambda_{1,\mathfrak{p}}, \psi_{1,\mathfrak{p}}); \ldots; (\phi_{r_\mathfrak{p},\mathfrak{p}}, \lambda_{r_\mathfrak{p},\mathfrak{p}}, \psi_{r_\mathfrak{p},\mathfrak{p}}); (\phi, \lambda, y - a)\right),$$

is a type which constitutes an OM representation of $F_\mathfrak{p}$ too.

The paths corresponding to the different OM representations computed by the Montes algorithm form a tree $\mathfrak{T}$ of types. The leaves of the tree each represent one prime factor of f in $\mathcal{O}_v[x]$. The number of connected components of this tree (i.e.

the number of root nodes) is in one-to-one correspondence with the set of prime factors of $\overline{f} = f \pmod{\mathfrak{m}}$ in $\mathbb{F}[y]$. For instance:

(5)



In this example we have three prime ideals, which all share a common first level. Additionally, the prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ share a common second level as well. Since the tree $\mathfrak{T}$ is connected, $\overline{f}$ is a power of the prime polynomial ψ_0 in $\mathbb{F}[y]$. The polynomials $F_\mathfrak{p}$, $F_\mathfrak{q}$ have Okutsu depth 2, while $F_\mathfrak{l}$ has depth 3.

Definition 2.2. *For two prime ideals $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$, the* index of coincidence $\ell = i(\mathfrak{p}, \mathfrak{q})$ *is the first different level of their respective types. More precisely, $\ell = 0$ if $\mathfrak{t}_\mathfrak{p}$ and $\mathfrak{t}_\mathfrak{q}$ have different root nodes. If $\psi_{0,\mathfrak{p}} = \psi_{0,\mathfrak{q}}$, then ℓ is minimal such that*

$$(\phi_{\ell,\mathfrak{p}}, \lambda_{\ell,\mathfrak{p}}, \psi_{\ell,\mathfrak{p}}) \neq (\phi_{\ell,\mathfrak{q}}, \lambda_{\ell,\mathfrak{q}}, \psi_{\ell,\mathfrak{q}}).$$

One advantage of OM representations of prime ideals, is that they yield explicit formulas for the $\mathfrak{p}$-valuation of the ϕ-polynomials at each level of the type $\mathfrak{t}_\mathfrak{q}$. The following proposition, extracted from [5, Thm. 3.1] and [6, Prop. 4.7], will be heavily used throughout the paper. It involves certain polynomials $\phi(\mathfrak{p}, \mathfrak{q}) \in \mathcal{O}[x]$ and certain *hidden slopes* $\lambda_\mathfrak{p}^\mathfrak{q}$, which are secondary data that have been conveniently stored along the running of the Montes algorithm [6, Sec. 4].

Proposition 2.3. *Let $\mathfrak{p} \in \mathcal{P}$ be a prime ideal of $\mathcal{O}_L$. Then for any $1 \leqslant i \leqslant r_\mathfrak{p} + 1$,*

$$w_\mathfrak{p}(\phi_{i,\mathfrak{p}}(\theta)) = \frac{V_{i,\mathfrak{p}} + \lambda_{i,\mathfrak{p}}}{e_{1,\mathfrak{p}} \cdots e_{i-1,\mathfrak{p}}},$$

where $V_{1,\mathfrak{p}} = 0$ and $V_{i+1,\mathfrak{p}} = e_{i,\mathfrak{p}} f_{i,\mathfrak{p}} (e_{i,\mathfrak{p}} V_{i,\mathfrak{p}} + h_{i,\mathfrak{p}})$ for all $1 \leqslant i \leqslant r_\mathfrak{p}$.

Let $\mathfrak{q} \in \mathcal{P}$ be another prime ideal such that $\mathfrak{p} \neq \mathfrak{q}$ and with index of coincidence $\ell = i(\mathfrak{p}, \mathfrak{q})$. For any $1 \leqslant i \leqslant r_\mathfrak{q} + 1$,

$$w_\mathfrak{p}(\phi_{i,\mathfrak{q}}(\theta)) = \begin{cases} 0, & \text{if } \ell = 0, \\ \dfrac{V_i + \lambda_i}{e_1 \cdots e_{i-1}}, & \text{if } i < \ell, \\ \dfrac{V_\ell + \lambda_\mathfrak{p}^\mathfrak{q}}{e_1 \cdots e_{\ell-1}}, & \text{if } i = \ell \text{ and } \phi_{\ell,\mathfrak{q}} = \phi(\mathfrak{p}, \mathfrak{q}), \\ \dfrac{m_{i,\mathfrak{q}}}{m_\ell} \cdot \dfrac{V_\ell + \operatorname{Min}\left\{\lambda_\mathfrak{p}^\mathfrak{q}, \lambda_\mathfrak{q}^\mathfrak{p}\right\}}{e_1 \cdots e_{\ell-1}}, & \text{otherwise.} \end{cases}$$

In these formulas, we omit the subscript $\mathfrak{p}$, $\mathfrak{q}$ when the invariants of the two types coincide.

Okutsu bases of the integral closure of $\mathcal{O}_v$. Let $L_\mathfrak{p}$ be the completion of L with respect to the $\mathfrak{p}$-adic topology. We may consider a topological embedding $L \subset L_\mathfrak{p} \subset \overline{K}_v$, so that $L_\mathfrak{p}$ may be identified to a finite extension of K_v of degree $n_\mathfrak{p}$. We denote by $\mathcal{O}_\mathfrak{p}$ the integral closure of $\mathcal{O}_v$ in $L_\mathfrak{p}$.

Let r be the Okutsu depth of $F_\mathfrak{p}$ and suppose that

$$\mathfrak{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_{r+1}, \lambda_{r+1}, \psi_{r+1})),$$

is the leaf corresponding to $F_{\mathfrak{p}}$ in the tree of an OM factorisation of f.

The Okutsu frame $[\phi_1, \dots, \phi_r]$ determines optimal polynomials $g_{0,\mathfrak{p}}, \dots, g_{n_{\mathfrak{p}}-1,\mathfrak{p}}$ in $\mathcal{O}[x]$ as follows. Each $0 \leqslant i < n_{\mathfrak{p}}$ may be expressed in a unique way as:

$$i = a_0 + a_1 m_1 + \cdots + a_r m_r, \qquad 0 \leqslant a_j < m_{j+1}/m_j = e_j f_j.$$

Thus, the polynomials:

$$g_{i,\mathfrak{p}} := x^{a_0} \prod_{j=1} \phi_j^{a_j}, \qquad 0 \leqslant i < n_{\mathfrak{p}},$$

are monic polynomials in $\mathcal{O}[x]$ of degree $\deg g_{i,\mathfrak{p}} = i$.

The following result is due to Okutsu [11].

Theorem 2.4. *For all $0 \leqslant i < n_{\mathfrak{p}}$, the rational number $w_{\mathfrak{p}}(g_{i,\mathfrak{p}}(\theta))$ is maximal amongst all monic polynomials in $\mathcal{O}_v[x]$ of degree i.*

By Theorem 1.4, we get a reduced triangular $\mathcal{O}_v$-basis of $\mathcal{O}_{\mathfrak{p}}$ by taking the images under the embedding $L \subset L_{\mathfrak{p}}$ of the elements:

$$\alpha_i := \pi^{-\lfloor w_{\mathfrak{p}}(g_{i,\mathfrak{p}}(\theta))\rfloor} g_{i,\mathfrak{p}}(\theta), \qquad 0 \leqslant i < n_{\mathfrak{p}}. \tag{6}$$

We call $(\alpha_i)_{0\leqslant i<n_{\mathfrak{p}}}$ the *Okutsu basis* of $\mathcal{O}_{\mathfrak{p}}$, or simply the Okutsu $\mathfrak{p}$-basis.

If f is irreducible in $\mathcal{O}_v[x]$, then $\mathcal{P} = \{\mathfrak{p}\}$ and $w = w_{\mathfrak{p}}$. Theorems 1.4 and 2.4 show that in this case, (6) is a reduced triangular v-integral basis of $\mathcal{O}_L$. Thus, from now on, we may assume that $\#\mathcal{P} > 1$.

For further purposes, the family of numerators of an Okutsu $\mathfrak{p}$-basis is extended by adding an Okutsu approximation to $F_{\mathfrak{p}}$,

$$\mathcal{N}_{\mathfrak{p}} := \left\{1 = g_{0,\mathfrak{p}}, \dots, g_{n_{\mathfrak{p}}-1,\mathfrak{p}}, g_{n_{\mathfrak{p}},\mathfrak{p}} := \phi_{\mathfrak{p}}\right\}. \tag{7}$$

Definition 2.5. *Let $S \subseteq \mathcal{P}$ be a subset of prime ideals of $\mathcal{O}_L$ and consider the Okutsu set*

$$\mathrm{Ok}(S) = \left\{ \prod_{\mathfrak{p}\in S} g_{i_{\mathfrak{p}},\mathfrak{p}} : 0 \leqslant i_{\mathfrak{p}} \leqslant n_{\mathfrak{p}} \right\} \subset \mathcal{O}[x],$$

of all polynomials that are a product of exactly one extended Okutsu $\mathfrak{p}$-numerator for each $\mathfrak{p} \in S$.

By construction, all polynomials in $\mathrm{Ok}(S)$ are monic. Note that the Okutsu set depends on the choice of an Okutsu approximation $\phi_{\mathfrak{p}} \approx F_{\mathfrak{p}}$ for each $\mathfrak{p} \in S$.

Theorem 2.6. *Let $h \in \mathcal{O}[x]$ be a monic polynomial of degree $0 \leqslant i < n_S$. For appropriate choices of the Okutsu approximations $\phi_{\mathfrak{p}}$, the set $\mathrm{Ok}(S)$ contains a polynomial g of degree i such that*

$$w_{\mathfrak{p}}(g(\theta)) \geqslant w_{\mathfrak{p}}(h(\theta)), \quad \forall\, \mathfrak{p} \in S.$$

This is one of the main results of the paper, whose proof will be postponed to Section 5.

Up to finding the right Okutsu approximations, Theorems 1.4 and 2.6 show that we may find a reduced triangular basis of $\mathcal{O}_L$ just by finding polynomials of degree $0, 1, \dots, n-1$, with maximal w-value in the finite set $\mathrm{Ok}(\mathcal{P})$ (c.f. Theorem 3.4).

Note that a brute force algorithm testing all possible factors $g_{i_{\mathfrak{p}},\mathfrak{p}}$ of the Okutsu bases leading to polynomials of a fixed degree i would be exponential.

A simple and very efficient algorithm, presented in Section 3, can be employed to choose an optimal combination of basis numerators for each degree i.

Okutsu bases of fractional ideals. Let I be a non-zero fractional ideal of $\mathcal{O}_L$,

$$I = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{a_\mathfrak{p}}$$

We consider a map giving a shifted valuation for a prime ideal $\mathfrak{p}$ as a factor of the fractional ideal I:

$$\begin{aligned} w_{\mathfrak{p},I} : L &\longrightarrow \mathbb{Q}\cup\{\infty\}, \\ \alpha &\longmapsto w_{\mathfrak{p},I}(\alpha) = w_\mathfrak{p}(\alpha) - a_\mathfrak{p}/e(\mathfrak{p}/\mathfrak{m}). \end{aligned}$$

Also, for a subset $S\subseteq\mathcal{P}$ we define:

$$w_{S,I}(\alpha) = \operatorname{Min}\{w_{\mathfrak{p},I}(\alpha) : \mathfrak{p}\in S\}.$$

Note that an element $\alpha\in L$ belongs to I if and only if $w_{\mathcal{P},I}(\alpha)\geqslant 0$.

Clearly these maps are consistent with the functions given in Definition 1.1, as $w_\mathfrak{p} = w_{\mathfrak{p},\mathcal{O}_L}$ and $w = w_{\mathcal{P},\mathcal{O}_L}$.

Definition 2.7. *Let I be a fractional ideal of $\mathcal{O}_L$. Let $S\subseteq\mathcal{P}$ be a subset of prime ideals of $\mathcal{O}_L$ and denote $n_S := \sum_{\mathfrak{p}\in S} n_\mathfrak{p}$. An Okutsu S-basis of I is a triangular family*

$$g_0(\theta)/\pi^{\lfloor\nu_0\rfloor}, \dots, g_{n_S-1}(\theta)/\pi^{\lfloor\nu_{n_S-1}\rfloor},$$

with numerators g_i in $\operatorname{Ok}(S)$ of degree i, such that $\nu_i = w_{S,I}(g_i(\theta)) \geqslant w_{S,I}(h(\theta))$ for all monic polynomials $h\in\mathcal{O}_v[x]$ of degree i, and for all $0\leqslant i < n_S$.

A result analogous to Theorem 1.4 holds: an Okutsu $\mathcal{P}$-basis of I is a reduced triangular basis of I as an $\mathcal{O}$-module. Also, Theorem 2.6 holds if we replace $w_\mathfrak{p}$ with $w_{\mathfrak{p},I}$, because both functions differ only in a constant shift. Therefore, just as for the maximal order, it makes sense to compute an Okutsu S-basis of I by looking for polynomials in $\operatorname{Ok}(S)$ with a maximal $w_{S,I}$-value amongst all polynomials in $\operatorname{Ok}(S)$ of a given degree. The MaxMin algorithm serves this purpose.

3. MaxMin

3.1. **Formal extension of the Okutsu $\mathfrak{p}$-bases.** The aim of the MaxMin algorithm is, given a set of prime ideals $S\subseteq\mathcal{P}$ and a fractional ideal I, to perform an efficient search for $w_{S,I}$-optimal polynomials in $\operatorname{Ok}(S)$.

To decide which numerators are chosen for each degree, we need only to know the values $w_\mathfrak{q}(g_{i_\mathfrak{p},\mathfrak{p}}(\theta))$ for all $\mathfrak{p},\mathfrak{q}\in S$ and $0\leqslant i_\mathfrak{p}\leqslant n_\mathfrak{p}$. As presented in Section 2, these values are given by invariants present in an OM factorisation $\mathfrak{T}$ of f. The exception is $w_\mathfrak{p}(\phi_\mathfrak{p})$, which can be arbitrarily large, depending on the choice of $\phi_\mathfrak{p}$ the Okutsu approximation to $F_\mathfrak{p}$.

For this reason, we do not choose a concrete polynomial $\phi_\mathfrak{p}$ beforehand, but rather run the algorithm as if $w_\mathfrak{p}(\phi_\mathfrak{p}(\theta))$ (formally) takes the value ∞.

Definition 3.1. *For all $\mathfrak{p}\in S$ we define the following function on the Okutsu set:*

$$w_\mathfrak{p} :\ \operatorname{Ok}(S)\longrightarrow\mathbb{Q}\cup\{\infty\},\quad g\longmapsto\begin{cases} w_\mathfrak{p}(g(\theta)), & \text{if } \phi_\mathfrak{p}\nmid g,\\ \infty, & \text{if } \phi_\mathfrak{p}\mid g.\end{cases}$$

This function does not depend on the choice of the Okutsu approximations $\phi_\mathfrak{p}$ as by Lemma 2.1 and Proposition 2.3 the value of $w_\mathfrak{q}(\phi_\mathfrak{p}(\theta))$ for $\mathfrak{q}\neq\mathfrak{p}$ only depends on $\mathfrak{p},\mathfrak{q}$ and not the choice of $\phi_\mathfrak{p}$. Thus, it makes sense to consider symbolic polynomials $\phi_\mathfrak{p}$ of degree $n_\mathfrak{p}$.

We consider a similar extension of the functions $w_{\mathfrak{p},I}$, $w_{S,I}$ to the Okutsu set:

$$w_{p,I}(g) := w_{\mathfrak{p}}(g) - a_{\mathfrak{p}}/e(\mathfrak{p}/\mathfrak{m}), \qquad w_{S,I}(g) := \operatorname{Min}\{w_{\mathfrak{p},I}(g) : \mathfrak{p} \in S\}.$$

We have $w_{S,I}(g) < \infty$ for all $g \in \operatorname{Ok}(S)$ with the exception of a single polynomial $\phi_S := \prod_{\mathfrak{p}\in S} \phi_{\mathfrak{p}}$. Also, $w_{S,I}(g) \geqslant w_{S,I}(g(\theta))$, and equality holds for adequate choices of all $\phi_{\mathfrak{p}}$ (depending on the given polynomial $g \in \operatorname{Ok}(S)$, $g \neq \phi_S$).

The algorithm will provide a recipe to construct polynomials $g_i \in \operatorname{Ok}(S)$ of degree i with a maximal value of $w_{S,I}(g_i)$ among all polynomials of degree i in $\operatorname{Ok}(S)$. The corresponding member of the triangular basis will be

$$\alpha_i = g_i(\theta)\pi^{-\lfloor w_{S,I}(g_i)\rfloor}, \qquad 0 \leqslant i < n_S.$$

For a practical computation of α_i, we must apply the Single-Factor Lifting algorithm [9] to find concrete Okutsu approximations $\phi_{\mathfrak{p}}$, with a value $w_{\mathfrak{p}}(\phi_{\mathfrak{p}}(\theta))$ large enough to guarantee that $w_{S,I}(g_i) = w_{S,I}(g_i(\theta))$ for all $0 \leqslant i < n_S$.

3.2. **The MaxMin algorithm.** For each type $\mathfrak{t}$ in the tree $\mathfrak{T}$, we denote by $S_{\mathfrak{t}} \subseteq S$ the subset of prime ideals $\mathfrak{p} \in S$ such that $\mathfrak{t}$ is one of the nodes in the path joining the leaf $\mathfrak{t}_{\mathfrak{p}}$ with its root node.

We fix an ordering $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ on the set S, with the property that for all types $\mathfrak{t}$ in $\mathfrak{T}$, the subset $S_{\mathfrak{t}} \subseteq S$ is an interval of S. That is, there exist indices $1 \leqslant a_{\mathfrak{t}} \leqslant b_{\mathfrak{t}} \leqslant s$ such that,

$$S_{\mathfrak{t}} = [a_{\mathfrak{t}}, b_{\mathfrak{t}}] := \{\mathfrak{p}_j : a_{\mathfrak{t}} \leqslant j \leqslant b_{\mathfrak{t}}\}. \tag{8}$$

As the branches of $\mathfrak{T}$ do not cross one-another, the reader will easily be convinced that it is always possible to consider such an ordering.

We consider multi-indices $\mathfrak{i} = (i_{\mathfrak{p}})_{\mathfrak{p}\in S}$ of degree $\deg \mathfrak{i} := \sum_{\mathfrak{p}} i_{\mathfrak{p}}$, leading to monic polynomials $g_{\mathfrak{i}} := \prod_{\mathfrak{p}} g_{i_{\mathfrak{p}},\mathfrak{p}} \in \mathcal{O}[x]$ in the Okutsu set $\operatorname{Ok}(S)$, with $\deg g_{\mathfrak{i}} = \deg \mathfrak{i}$.

Definition 3.2. *A multi-index $\mathfrak{i} = (i_{\mathfrak{p}})_{\mathfrak{p}\in S}$ is said to be* maximal *if*

$$w_{S,I}(g_{\mathfrak{i}}) \geqslant w_{S,I}(g_{\mathfrak{j}}),$$

for all multi-indices $\mathfrak{j}$ with $\deg \mathfrak{j} = \deg \mathfrak{i}$.

In this case, we also say that $g_{\mathfrak{i}}$ is a maximal numerator.

Notation. *For $1 \leqslant j \leqslant s$ we denote by $\mathfrak{u}_j$ the multi-index with coordinates $i_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \neq \mathfrak{p}_j$ and $i_{\mathfrak{p}_j} = 1$.*

Algorithm 1 MaxMin[S] algorithm

Input: A fractional ideal I of $\mathcal{O}_L$ and Okutsu numerators $\{g_{i,\mathfrak{p}} : 0 \leqslant i \leqslant n_{\mathfrak{p}}\}$ of $\mathfrak{p}$-bases for each $\mathfrak{p} \in S$.

Output: A family $\mathfrak{i}_0, \mathfrak{i}_1, \dots, \mathfrak{i}_{n_S} \in \mathbb{N}^s$ of multi-indices of degree $0, 1, \dots, n$ respectively.

1: $\mathfrak{i}_0 \leftarrow (0, \dots, 0)$
2: **for** $k = 0 \to n_S - 1$ **do**
3: $\quad j \leftarrow \operatorname{Min}\{1 \leqslant i \leqslant s : w_{\mathfrak{p}_i,I}(g_{\mathfrak{i}_k}) = w_{S,I}(g_{\mathfrak{i}_k})\}$
4: $\quad \mathfrak{i}_{k+1} \leftarrow \mathfrak{i}_k + \mathfrak{u}_j$
5: **end for**

The next result is the second fundamental result in the paper. Its proof will be given in Section 6.

Theorem 3.3. *All output multi-indices of* MaxMin *are maximal.*

This gives the name MaxMin for the algorithm, because it finds the maximal value amongst the minima of certain numerical data. This provides a computation of a reduced triangular basis as follows.

Theorem 3.4. *Let* $\mathbb{i}_0, \mathbb{i}_1, \ldots, \mathbb{i}_{n_S}$ *be an output of* MaxMin. *Choose Okutsu approximations* $\phi_{\mathfrak{p}}$ *of all* $\mathfrak{p} \in \mathcal{P}$, *such that*

$$w_{S,I}\left(g_{\mathbb{i}_k}\right) = w_{S,I}\left(g_{\mathbb{i}_k}(\theta)\right), \qquad 0 \leqslant k < n_S.$$

Then, $g_{\mathbb{i}_0}, g_{\mathbb{i}_1}, \ldots, g_{\mathbb{i}_{n-1}}$ *are numerators of an Okutsu* S*-basis of* I.

Proof. Let $h \in \mathcal{O}_v[x]$ be a monic polynomial of degree $0 \leqslant k < n_S$. By Theorem 2.6, there exists $g \in \mathrm{Ok}(S)$ (for adequate choices of all $\phi_{\mathfrak{p}}$ for $\mathfrak{p} \in S$) of degree k such that $w_{S,I}\left(g(\theta)\right) \geqslant w_{S,I}\left(h(\theta)\right)$.

On the other hand, regardless of the choices of the $\phi_{\mathfrak{p}}$, we have $w_{S,I}\left(g_{\mathbb{i}_k}\right) \geqslant w_{S,I}\left(g\right)$ by the maximality of $\mathbb{i}_k$. Hence,

$$w_{S,I}\left(g_{\mathbb{i}_k}(\theta)\right) = w_{S,I}\left(g_{\mathbb{i}_k}\right) \geqslant w_{S,I}\left(g\right) \geqslant w_{S,I}\left(g(\theta)\right) \geqslant w_{S,I}\left(h(\theta)\right). \qquad \square$$

We will now present some remarks about the behaviour of the algorithm. We assume $I = \mathcal{O}_L$ for simplicity.

3.2.1. *Guaranteed termination.* MaxMin always terminates after exactly n_S iterations.

Thanks to the convention $w_{\mathfrak{p}}(\phi_{\mathfrak{p}}) = \infty$, the index j in step 3 indicates a prime $\mathfrak{p}_j$ such that for the multi-index $\mathbb{i}_k = (i_{\mathfrak{p}})_{\mathfrak{p}\in S}$, we will always have $i_{\mathfrak{p}_j} < n_{\mathfrak{p}_j}$. Thus, the next multi-index $\mathbb{i}_{k+1} = (i'_{\mathfrak{p}})_{\mathfrak{p}\in S}$ constructed in step 4 has indices $i'_{\mathfrak{p}} \leqslant n_{\mathfrak{p}}$ for all $\mathfrak{p}$.

Furthermore, the first and last output multi-indices are $\mathbb{i}_0 = (0, \ldots, 0)$ and $\mathbb{i}_{n_s} = (n_{\mathfrak{p}_1}, \ldots, n_{\mathfrak{p}_s})$. As such, $g_{\mathbb{i}_0} = 1$ and $g_{\mathbb{i}_{n_S}} = \prod_{\mathfrak{p}\in S} \phi_{\mathfrak{p}}$.

3.2.2. *Polynomial products are not computed.* The algorithm does not compute the products $g_{\mathbb{i}_k}$. It only computes the values $w_{\mathfrak{p}}(g_{\mathbb{i}_k})$ for all $\mathfrak{p} \in S$, which are determined by the 3-dimensional array of data $w_{\mathfrak{p}_k}(g_{j_i,\mathfrak{p}_i})$ indexed by i, j_i, and k in the ranges $1 \leqslant i \leqslant s$, $0 \leqslant j_i \leqslant n_{\mathfrak{p}_i}$, and $1 \leqslant k \leqslant s$, respectively.

3.2.3. *MaxMin is not a universal maximiser.* If the numbers $w_{\mathfrak{p}_k}(g_{j_i,\mathfrak{p}_i})$ are replaced by arbitrary, non-negative rational numbers $\nu_{k,j_i,i} \in \mathbb{Q}_{>0}$ and we take

$$\nu_{k,\mathbb{i}} := \sum_{i=1}^{s} \nu_{k,j_i,i},$$

with $\mathbb{i} = (j_i)_{1\leqslant i\leqslant s}$ a multi-index as above, the MaxMin routine may fail to compute

$$\mathrm{Max}\left\{\mathrm{Min}\left\{\nu_{k,\mathbb{i}} : 1 \leqslant k \leqslant s\right\} : \deg \mathbb{i} = d\right\},$$

a maximal multi-index of degree d.

3.2.4. *Initial conditions.* Suppose $\mathbb{i} = (i_{\mathfrak{p}})_{\mathfrak{p}\in S}$ is a multi-index with degree $\deg \mathbb{i} = d$, such that $w_{S,I}(g_{\mathbb{i}})$ is maximal amongst all multi-indices of degree d. Then, it may not be true that by increasing an adequate index by one, we get a multi-index $\mathbb{j}$, of degree $d+1$, which renders a maximal value of $w(g_{\mathbb{j}})$ amongst all multi-indices of degree $k+1$.

For instance, let us consider the example presented in Section 3.3. The output index of degree 3 is $\mathbb{i}_3 = (1,2,0)$, resulting in the polynomial $g_3 = \phi_{1,\mathfrak{p}}\phi_{1,\mathfrak{q}}^2$ with valuation vector $\vec{w}(g_3) = (18,12,12)$ for $w_{\mathfrak{p}}$, $w_{\mathfrak{q}}$ and $w_{\mathfrak{l}}$ respectively.

We could choose an alternative index $\mathbb{j}_3 = (1,1,1)$ which would give a polynomial $g_3' = \phi_{1,\mathfrak{p}}\phi_{1,\mathfrak{q}}\phi_{1,\mathfrak{l}}$ with the exact same valuations $\vec{w}(g_3') = (18,12,12)$. However, none of the indices $(2,1,1)$, $(1,2,1)$, $(1,1,2)$ is maximal. For instance, $\mathbb{j}_4 = (1,2,1)$ determines the polynomial $g_4' = \phi_{1,\mathfrak{p}}\phi_{1,\mathfrak{q}}^2\phi_{1,\mathfrak{l}}$ with valuations $\vec{w}(g_4') = (24,16,16)$. This is clearly not maximal as the polynomial constructed by MaxMin $g_4 = \phi_{1,\mathfrak{p}}\phi_{2,\mathfrak{q}}$ has valuations $\vec{w}(g_4) = (18,22,21)$.

It is remarkable that the extremely simple strategy that MaxMin employs to choose successive maximal multi-indices is able to avoid these pathological cases.

3.2.5. *Ordering of input prime ideals.* Theorem 3.3 shows that MaxMin produces a sequence of maximal multi-indices regardless of the choice of ordering on S, as long as it satisfies (8). However, the numerators $g_{\mathbb{i}_k}$ produced from these multi-indices do depend on the choice of ordering.

3.2.6. *Complexity.* To compute a triangular v-integral basis of L, a number of steps are required:

(1) Use the Montes algorithm to produce an OM representation $\mathfrak{T}$ of f.
(2) Run MaxMin$[\mathcal{P}]$ to generate a family of maximal indices $\mathbb{i}_0, \ldots, \mathbb{i}_{n-1}$.
(3) Apply the Single Factor Lifting algorithm from [9] to get an adequate improvement of the Okutsu approximation of each prime factor of f.
(4) Compute the numerators of the Okutsu basis $g_0, \ldots, g_{n-1}$ specified by the maximal indices.
(5) Divide the Okutsu numerators by the appropriate power of π to create an integral basis.

The total complexity is equivalent to that of other OM based routines and is given in the following result.

Theorem 3.5 ([13, Thm. 6.1])**.** *Suppose that $\mathbb{F}$ is a finite field with q elements and f is a separable polynomial. Take $\delta := v(\mathrm{disc}(f))$. The total cost of the computation of a v-integral basis of L by the application of the Montes and the MaxMin algorithms is*

$$O\left(n^{2+\epsilon}\delta^{1+\epsilon} + n^{1+\epsilon}\delta\log(q) + n^{1+\epsilon}\delta^{2+\epsilon}\right),$$

operations in $\mathbb{F}$. If we assume q small, this will give us a refined estimation of $O\left(n^{2+\epsilon}\delta^{1+\epsilon} + n^{1+\epsilon}\delta^{2+\epsilon}\right)$ bit operations.

3.3. **MaxMin example.** We will now present a small example for $I = \mathcal{O}_L$ and $S = \mathcal{P} = \{\mathfrak{p}, \mathfrak{q}, \mathfrak{l}\}$, where $\mathfrak{T}$ is connected. The tree is shown in Figure 1, where we indicate only the data (ϕ, λ) for each edge.

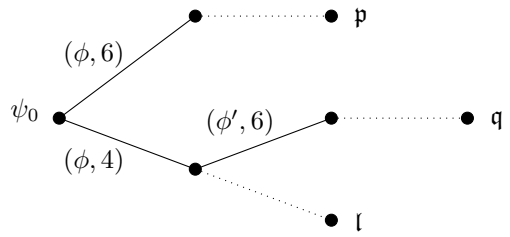


FIGURE 1. Example connected tree $\mathfrak{T}$ of types.

Since all slopes have integer values, all denominators e_i are equal to one. We assume that $f_0 = m_1 = \deg \psi_0 = 1$ and:

$$\begin{aligned}
\mathfrak{p}: &\quad e_1 = 1, f_1 = 4, h_1 = 6;\\
\mathfrak{q}: &\quad e_1 = 1, f_1 = 3, h_1 = 4; \quad e_2 = 1, f_2 = 2, h_2 = 6;\\
\mathfrak{l}: &\quad e_1 = 1, f_1 = 3, h_1 = 4.
\end{aligned}$$

Note that $n_{\mathfrak{p}} = 4$, $n_{\mathfrak{q}} = 6$, and $n_{\mathfrak{l}} = 3$, so that $n = 13$.

The data corresponding to the edges leading to a leaf are not specified as we do not need them to run MaxMin.

Suppose moreover that

$$\phi(\mathfrak{p}, \mathfrak{q}) = \phi(\mathfrak{p}, \mathfrak{l}) = \phi_{1,\mathfrak{p}} = \phi_{1,\mathfrak{q}} = \phi_{1,\mathfrak{l}} = \phi, \qquad \phi(\mathfrak{q}, \mathfrak{l}) = \phi_{2,\mathfrak{q}} = \phi',$$

and the hidden slopes are:

$$\lambda^{\mathfrak{q}}_{\mathfrak{p}} = \lambda^{\mathfrak{l}}_{\mathfrak{p}} = 6, \qquad \lambda^{\mathfrak{p}}_{\mathfrak{q}} = \lambda^{\mathfrak{p}}_{\mathfrak{l}} = 4, \qquad \lambda^{\mathfrak{l}}_{\mathfrak{q}} = 6, \qquad \lambda^{\mathfrak{q}}_{\mathfrak{l}} = 5.$$

The numerators of the extended Okutsu bases of each prime ideal will be,

$$\begin{aligned}
\mathcal{N}_{\mathfrak{p}}: &\ 1,\ \phi_{1,\mathfrak{p}},\ \phi^2_{1,\mathfrak{p}},\ \phi^3_{1,\mathfrak{p}},\ \phi_{\mathfrak{p}};\\
\mathcal{N}_{\mathfrak{q}}: &\ 1,\ \phi_{1,\mathfrak{q}},\ \phi^2_{1,\mathfrak{q}},\ \phi_{2,\mathfrak{q}},\ \phi_{2,\mathfrak{q}}\phi_{1,\mathfrak{q}},\ \phi_{2,\mathfrak{q}}\phi^2_{1,\mathfrak{q}},\ \phi_{\mathfrak{q}};\\
\mathcal{N}_{\mathfrak{l}}: &\ 1,\ \phi_{1,\mathfrak{l}},\ \phi^2_{1,\mathfrak{l}},\ \phi_{\mathfrak{l}}.
\end{aligned}$$

Using the explicit formulas of Proposition 2.3, we may compute the valuations of each of the ϕ-polynomials. We write them as a tuple $\vec{w} = (w_{\mathfrak{p}}, w_{\mathfrak{q}}, w_{\mathfrak{l}})$.

$$\begin{aligned}
&\vec{w}(\phi_{1,\mathfrak{p}}) = (6,4,4), \qquad \vec{w}(\phi_{\mathfrak{p}}) = (\infty, 16, 16),\\
&\vec{w}(\phi_{1,\mathfrak{q}}) = (6,4,4), \qquad \vec{w}(\phi_{2,\mathfrak{q}}) = (12,18,17) \qquad \vec{w}(\phi_{\mathfrak{q}}) = (24,\infty,34),\\
&\vec{w}(\phi_{1,\mathfrak{l}}) = (6,4,4), \qquad \vec{w}(\phi_{\mathfrak{l}}) = (12,17,\infty).
\end{aligned}$$

We can now step through the results of running MaxMin. The "minimal" valuation is underlined at each step. This indicates the index which will be incremented in the following step.

i	g_i	$\vec{w}(g_i)$	$w(g_i)$
0	$1 \cdot 1 \cdot 1$	$(\underline{0}, 0, 0)$	0
1	$\phi_{1,\mathfrak{p}} \cdot 1 \cdot 1$	$(6, \underline{4}, 4)$	4
2	$\phi_{1,\mathfrak{p}} \cdot \phi_{1,\mathfrak{q}} \cdot 1$	$(12, \underline{8}, 8)$	8
3	$\phi_{1,\mathfrak{p}} \cdot \phi^2_{1,\mathfrak{q}} \cdot 1$	$(18, \underline{12}, 12)$	12
4	$\phi_{1,\mathfrak{p}} \cdot \phi_{2,\mathfrak{q}} \cdot 1$	$(\underline{18}, 22, 21)$	18
5	$\phi^2_{1,\mathfrak{p}} \cdot \phi_{2,\mathfrak{q}} \cdot 1$	$(\underline{24}, 26, 25)$	24
6	$\phi^3_{1,\mathfrak{p}} \cdot \phi_{2,\mathfrak{q}} \cdot 1$	$(30, 30, \underline{29})$	29

7	$\phi_{1,\mathfrak{p}}^3 \cdot \phi_{2,\mathfrak{q}} \cdot \phi_{1,\mathfrak{l}}$	$(36, 34, \underline{33})$	33
8	$\phi_{1,\mathfrak{p}}^3 \cdot \phi_{2,\mathfrak{q}} \cdot \phi_{1,\mathfrak{l}}^2$	$(42, 38, \underline{37})$	37
9	$\phi_{1,\mathfrak{p}}^3 \cdot \phi_{2,\mathfrak{q}} \cdot \phi_{\mathfrak{l}}$	$(\underline{42}, 47, \infty)$	42
10	$\phi_{\mathfrak{p}} \cdot \phi_{2,\mathfrak{q}} \cdot \phi_{\mathfrak{l}}$	$(\infty, \underline{51}, \infty)$	51
11	$\phi_{\mathfrak{p}} \cdot \phi_{2,\mathfrak{q}} \phi_{1,\mathfrak{q}} \cdot \phi_{\mathfrak{l}}$	$(\infty, \underline{55}, \infty)$	55
12	$\phi_{\mathfrak{p}} \cdot \phi_{2,\mathfrak{q}} \phi_{1,\mathfrak{q}}^2 \cdot \phi_{\mathfrak{l}}$	$(\infty, \underline{59}, \infty)$	59
13	$\phi_{\mathfrak{p}} \cdot \phi_{\mathfrak{q}} \cdot \phi_{\mathfrak{l}}$	(∞, ∞, ∞)	∞

The final element g_{13} is not included in the v-integral basis.

4. Computational examples

In this section, we will present a number of example computations using an implementation of the MaxMin algorithm for the computer algebra system Magma [2]. We compare MaxMin's execution time for computing v-integral bases with that of the method of the quotients, another OM-based algorithm, as well as the internal routines found in Magma.

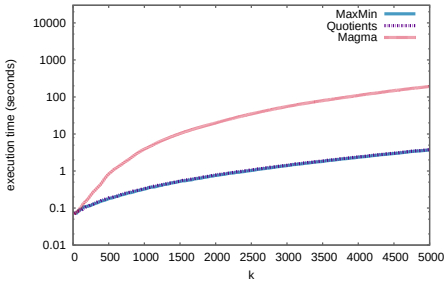
All executions were performed on GNU/Linux running on 8-core 3.0GHz nodes with 32GB main memory. Each execution ran in a single core, using Magma 2.18-5.

Examples will be given for number fields $L = \mathbb{Q}[x]/(f)$ for polynomials $f \in \mathbb{Z}[x]$ and function fields $L = \mathbb{F}_q(t)[x]/(f)$ over a finite field $\mathbb{F}_q$ for polynomials $f \in \mathbb{F}_q[t][x]$. The example defining polynomials are taken from [9].

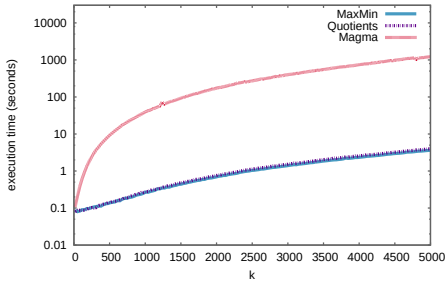
The first example is comprised of the B-class of polynomials,

$$B_{p,k}(x) = (x^2 - 2x + 4)^3 + p^k,$$

of degree 6. We take $f(x) = B_{13,k}(x) \in \mathbb{Z}[x]$ in the number field case and $f(x) = B_{t^3+2,k}(x) \in \mathbb{F}_7[t, x]$ in the function field case, with $k \leqslant 5000$. The execution times for computing a Hermitian v-integral basis of L are shown in Figure 2.



$B_{13,k}(x) \in \mathbb{Z}[x]$.



$B_{t^3+2,k}(x) \in \mathbb{F}_7[t, x]$.

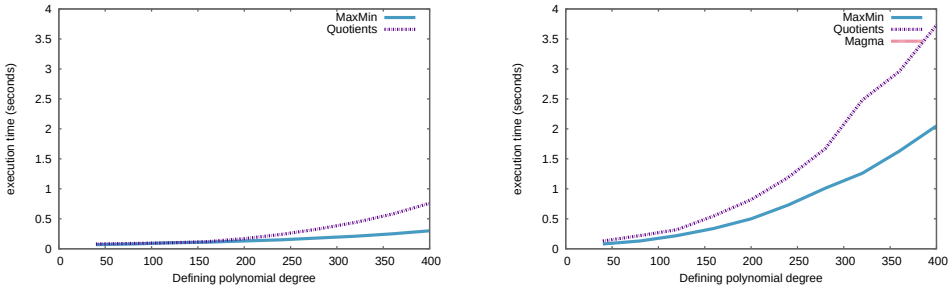
Figure 2. Running time for maximal order Hermitian p-basis computation defined by polynomials $B_{p,k}(x)$ with $k \leqslant 5000$.

Due to the low degree of the field extensions, computing the HNF of a basis is negligible compared to computing the basis itself. It can be seen that both OM-based routines have a similar performance and are roughly 100 times faster than the internal Magma routines in the number field case for $k = 5000$ and 1000 times faster in the function field case.

In order to demonstrate the performance of MaxMin on larger polynomials, we will consider the A-class of polynomials

$$A^m_{p,n,k}(x) = (x^n + 2p^k)((x+2)^n + 2p^k)\cdots((x+2m-2)^n + 2p^k) + 2p^{nmk}.$$

These polynomials have degree nm. In the number field case, we take $f(x) = A^4_{101,n,29}(x) \in \mathbb{Z}[x]$ with $n \leqslant 100$. Figure 3 shows the times for the OM-based methods and the total times when we include the time to compute the Hermitian basis.

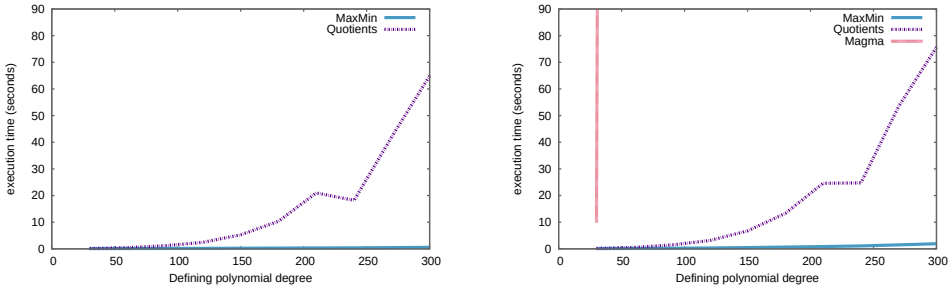


Without HNF. With HNF.

FIGURE 3. Running time for maximal order p-basis computation defined by polynomials $A^4_{101,n,29}(x)$ with $\deg(A^4_{101,n,29}) \leqslant 400$.

From this example, we can see that MaxMin is somewhat faster than the Method of the Quotients, however when the time to compute the HNF of the resulting basis is included, we see the advantage of the triangular basis computed by MaxMin. In this example, Magma took 257 seconds to compute the basis for $\deg f = 40$ (and does not appear in the figure), and was unable to complete the computation for $\deg f = 80$ due to main memory limitations.

We consider a slightly smaller example in the function field case, with $f(x) = A^3_{t^2+2,n,6} \in \mathbb{F}_7[t,x]$, once again for $n \leqslant 100$. The resulting execution times are presented in Figure 4.



Without HNF. With HNF.

FIGURE 4. Running time for maximal order p-basis computation defined by polynomials $A^3_{101,n,29}(x)$ with $\deg(A^4_{101,n,29}) \leqslant 400$.

Here, MaxMin computes a basis considerably faster than the Method of the Quotients, however the improvement in computing the HNF from the triangular basis is not as pronounced as in the number field case. The second data point for the Magma routine is at $\deg f = 60$, which took 3304 seconds to compute a Hermitian basis.

Finally, we will consider some very large examples. We take the recursively defined EC-class polynomials defined in this case as $EC_{p,j}(x) = E_{p,j}(x) \cdot C_{p,28} + p^{900}$, where the E-class and C-class polynomials are given in [9]. Firstly, we consider $f(x) = EC_{101,8}(x) \in \mathbb{Z}[x]$, a degree 900 polynomial which splits into six degree 6 factors and one degree 864 factor over the p-adics. Secondly, we consider $f(x) = EC_{t^2+4,4}(x) \in \mathbb{F}_7[t,x]$, a degree 72 polynomial that splits into four degree 9 factors and one degree 36 factor over the $p(t)$-adics.

TABLE 1. Running time (in seconds) for maximal order p-basis computation defined by polynomials $EC_{p,j}$.

$EC_{101,8}(x) \in \mathbb{Z}[x]$.

Algorithm	*Basis*	*HNF basis*
MaxMin	9.9	112.6
Quotients	21.1	429.3

$EC_{t^2+4,4}(x) \in \mathbb{F}_7[t,x]$.

Algorithm	*Basis*	*HNF basis*
MaxMin	13.3	21.5
Quotients	89.5	8353.8

These final examples show advantages of using MaxMin to compute a local basis, whether or not a subsequent step to pass the basis to HNF is required. However, they also illustrate the advantages of using a triangular basis instead of a basis in HNF where it is possible.

5. Optimal polynomials in the Okutsu set

In this section, we will present the additional details necessary to prove Theorem 2.6. This will be broken into two parts, Proposition 5.16 and Proposition 5.23, which together prove the theorem.

5.1. **Operators associated with a type.** Consider a type $\mathfrak{t}$ of order r over (K, v):

$$\mathfrak{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r)) .$$

The type $\mathfrak{t}$ carries three kinds of operators. There are normalised valuations:

$$v_i : K_v[x] \longrightarrow \mathbb{Z} \cup \{\infty\} , \qquad 0 \leqslant i \leqslant r.$$

The last valuation v_r is also denoted $v_{\mathfrak{t}}$. Also, we have Newton polygon operators:

$$\mathrm{N}_i = \mathrm{N}_{v_{i-1},\phi_i} : K_v[x] \longrightarrow 2^{\mathbb{R}^2}, \qquad 1 \leqslant i \leqslant r,$$

where $2^{\mathbb{R}^2}$ is the set of subsets of $\mathbb{R}^2$. The image of 0 is the empty set. For every non-zero $g \in K[x]$ we consider the canonical ϕ_i-expansion $g = \sum_{0 \leqslant s} a_s \phi_i^s$, where $a_s \in K[x]$ have degree less than $\deg \phi_i$. Then $\mathrm{N}_i(g)$ is the lower convex hull of the set of points $(s, v_{i-1}(a_s \phi_i^s))$.

Finally, we have residual polynomial operators:

$$\mathrm{R}_i = \mathrm{R}_{v_{i-1},\phi_i,\lambda_i} : K_v[x] \longrightarrow \mathbb{F}_i[y], \qquad 0 \leqslant i \leqslant r,$$

which are multiplicative: $\mathrm{R}_i(gh) = \mathrm{R}_i(g)\,\mathrm{R}_i(h)$ for all $g, h \in K[x]$.

The valuation v_0 is defined as

$$v_0\left(\sum_{0\leqslant s} a_s x^s\right) = \operatorname{Min}\left\{v\left(a_s\right) : 0 \leqslant s\right\}.$$

The residual polynomial operator R_0 is defined as:

$$\mathrm{R}_0(g) = \pi^{-v_0(g)} g(y) \pmod{\mathfrak{m}[y]}.$$

For $1 \leqslant i \leqslant r$ the operators v_i, R_i are defined in a certain recurrent way [8, Sec. 3.1].

Definition 5.1. *We say that* $\mathbb{t}$ *is* optimal *if* $m_1 < m_2 < \cdots < m_r$.

Definition 5.2. *Let* $\mathbb{t}$ *be a type of order* $r \geqslant 0$ *and* $g \in K_v[x]$. *We define* $\operatorname{ord}_{\mathbb{t}}(g)$ *as the non-negative integer* $\operatorname{ord}_{\psi_r}(\mathrm{R}_r(g))$ *where* ψ_r *and* $\mathrm{R}_r(g)$ *are considered as polynomials in* $\mathbb{F}_r[y]$. *If* $\operatorname{ord}_{\mathbb{t}}(g) > 0$ *we say that* $\mathbb{t}$ divides g *and we write* $\mathbb{t} \mid g$.

Definition 5.3. *Let* $\mathbb{t}$ *be a type of order* r *and* $g \in \mathcal{O}[x]$. *We say that* g *is a* representative *of* $\mathbb{t}$ *if* g *is a monic polynomial of degree* $m_{r+1} := e_r f_r m_r$ *such that* $\mathrm{R}_r(g) = \psi_r$. *We denote by* $\operatorname{Rep}(\mathbb{t})$ *the set of representatives of* $\mathbb{t}$.

If $\phi \in \mathcal{O}[x]$ is a representative of $\mathbb{t}$, then by definition $\tilde{\mathbb{t}} = (\mathbb{t}; (\phi, \lambda, \psi))$ is a type of order $r+1$ for any choice of a positive rational number λ and a monic irreducible polynomial $\psi \in \mathbb{F}_{r+1}[y]$, $\psi \neq y$.

Definition 5.4. *A* prime polynomial *is a monic irreducible polynomial in* $\mathcal{O}_v[x]$.

Since R_r is multiplicative and ψ_r is irreducible, the representatives of $\mathbb{t}$ are prime polynomials.

The next result collects the essential properties of the polynomials which are divisible by a type. It is taken from [5, Lem. 1.4, Thms. 3.1, 3.7].

Theorem 5.5. *Let* $\mathbb{t}$ *be a type of order* $r \geqslant 0$ *and let* $\phi \in \mathcal{O}[x]$ *be a representative of* $\mathbb{t}$. *Let* $F \in \mathcal{O}_v[x]$ *be a prime polynomial and choose* $\theta \in \overline{K}_v$ *a root of* F.

If $\phi \neq F$ *and* $\mathbb{t} \mid F$, *then*

1. $\mathrm{N}_{v_r,\phi}(F)$ *is one-sided of slope* $-\lambda$, *for a certain positive rational number* λ *such that* $v\left(\phi(\theta)\right) = (V_{r+1} + \lambda)/(e_1 \cdots e_r)$.
2. $\deg(F) = \deg(\phi^\ell)$, *where* $\ell = \ell(\mathrm{N}_{v_r,\phi}(F))$ *is the* length *of the Newton polygon; that is the abscissa of the right end point.*
3. $\deg(\mathrm{R}_{v_r,\phi,\lambda}(F)) = e_\lambda^{-1}\ell$ *and* $\mathrm{R}_{v_r,\phi,\lambda}(F) = \psi^a$, *where* e_λ *is the least positive denominator of* λ *and* $\psi \in \mathbb{F}_{r+1}[y]$ *is a monic irreducible polynomial* $\psi \neq y$.
4. *The type* $\tilde{\mathbb{t}} = (\mathbb{t}; (\phi, \lambda, \psi))$ *divides* F.

For $0 \leqslant i \leqslant r$, let $\mathbb{t}_i = \operatorname{Trunc}_i(\mathbb{t})$ be the type of order i obtained by dropping all levels $(\phi_j, \lambda_j, \psi_j)$ of order $j > i$ from $\mathbb{t}$.

By the definition of a type, each ϕ_i is a representative of $\mathbb{t}_{i-1}$, for $1 \leqslant i \leqslant r$.

The next result follows easily from Theorem 5.5 and [5, Lem. 2.4].

Theorem 5.6. *With the above notation,* $\mathbb{t}_i \mid F$ *for all* $0 \leqslant i \leqslant r$, $\mathrm{N}_i(F)$ *is one sided of slope* $-\lambda_i$, *and* $\mathrm{R}_i(F)$ *is a power of* ψ_i.

Finally, the following result follows from Theorem 5.5 and [5, Prop. 3.5].

Theorem 5.7. *With the above notation, let $g \in \mathcal{O}_v[x]$ be another prime polynomial such that $\mathfrak{t} \mid g$, $\tilde{\mathfrak{t}} \nmid g$. Then,*

$$v\left(g(\theta)\right) = \frac{\deg(g)}{\deg(\phi)} \frac{V_{r+1} + \operatorname{Min}\{\lambda, \lambda'\}}{e_1 \cdots e_r},$$

where $-\lambda'$ is the slope of $\mathrm{N}_{v_r,\phi}(g)$.

5.2. **Non-optimised tree of types.** Let us briefly describe how the Montes algorithm constructs the tree $\mathfrak{T}$ of OM representations of the prime factors of the input polynomial $f \in \mathcal{O}[x]$. Initially, $\overline{f}$ is factorised in $\mathbb{F}[y]$. For each monic irreducible factor φ of $\overline{f}$, a triplet $(\mathfrak{t}, \phi, \omega)$ is considered, where $\mathfrak{t} = (\varphi)$ is the type of order 0 determined by φ, ϕ is a representative of $\mathfrak{t}$ (that is, a monic lift of φ to $\mathcal{O}[x]$), and $\omega = \operatorname{ord}_{\mathfrak{t}}(f) = \operatorname{ord}_{\varphi}(\overline{f})$. All these triplets $(\mathfrak{t}, \phi, \omega)$ are stored in a stack.

Along the execution of the algorithm the stack always contains triplets $(\mathfrak{t}, \phi, \omega)$, where $\mathfrak{t} \mid f$, ϕ is a representative of $\mathfrak{t}$ and $\omega = \operatorname{ord}_{\mathfrak{t}}(f)$. The main loop of the algorithm takes such a triplet and attaches to the type $\mathfrak{t}$ one or more branches $\mathfrak{t}_{\lambda,\psi} := (\mathfrak{t}; (\phi, \lambda, \psi))$ of $\mathfrak{t}$ such that $\mathfrak{t}_{\lambda,\psi} \mid f$ and the pairs (λ, ψ) are considered as follows,

- $-\lambda$ runs on the slopes of $\mathrm{N}^{\omega}_{v_{\mathfrak{t}},\phi}(f) := \mathrm{N}_{v_{\mathfrak{t}},\phi}(f) \cap ([0, \omega] \times \mathbb{R})$.
- ψ runs on the prime factors of $\mathrm{R}_{v_{\mathfrak{t}},\phi,\lambda}(f)$.

Let $\phi_{\lambda,\psi} \in \mathcal{O}[x]$ be a representative of $\mathfrak{t}_{\lambda,\psi}$ and take $\omega_{\lambda,\psi} = \operatorname{ord}_{\psi}(\mathrm{R}_{v_{\mathfrak{t}},\phi,\lambda}(f)) = \operatorname{ord}_{\mathfrak{t}_{\lambda,\psi}}(f)$. If this positive integer is equal to one, then $\mathfrak{t}_{\lambda,\psi}$ divides only one of the prime factors $F_{\mathfrak{p}}$ of f in $\mathcal{O}_v[x]$. In this case, we add a final level to $\mathfrak{t}$ to construct the leaf $\mathfrak{t}_{\mathfrak{p}}$ associated with this prime factor. On the other hand, if $\omega_{\lambda,\psi} > 1$, then the triplet $(\mathfrak{t}_{\lambda,\psi}, \phi_{\lambda,\psi}, \omega_{\lambda,\psi})$ is pushed back onto the stack to bare further branching in future iterations of the main loop.

After a finite number of iterations of this process, the algorithm outputs a list $\mathfrak{t}_1, \ldots, \mathfrak{t}_N$ of types parametrising the prime factors of f in $\mathcal{O}_v[x]$. Let us denote by $\mathfrak{T}^{\mathrm{nop}}$ the tree of types obtained by this procedure. Note that for every node $\mathfrak{t} \in \mathfrak{T}^{\mathrm{nop}}$ which is not a leaf, the edges with left end point $\mathfrak{t}$ have the same ϕ-polynomial; a tree of types with this property is said to be *coherent*.

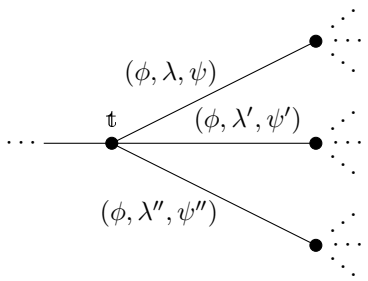


FIGURE 5. A segment of the non-optimised tree $\mathfrak{T}^{\mathrm{nop}}$.

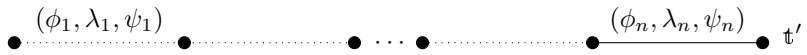
This describes a kind of "non-optimised" Montes algorithm, yielding a "non-optimised" tree of types. The types $\mathfrak{t}_{\lambda,\psi}$ may not be optimal. In fact, if $\lambda \in \mathbb{Z}$ and $\deg \psi = 1$, we have

$$\deg \phi_{\lambda,\psi} = e_{\lambda} \cdot \deg \psi \cdot \deg \phi = \deg \phi,$$

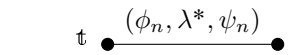
where e_λ is the positive denominator of λ. We must avoid this situation, because the numerical data attached to the types will not be intrinsic data of the prime factors of f.

For this reason, the Montes algorithm includes a "refinement procedure" which ensures that it only stores optimal types. However, a price must be paid; the output tree of OM representations is no longer coherent.

The optimised tree of OM representations (the real output of the Montes algorithm) may be derived from the non-optimised tree by an iterative application of the following transformation. Any path,

(9) 

in which all edges except for the final one are bad edges satisfying $\lambda_i \in \mathbb{Z}$, $\deg \psi_i = 1$ for $1 \leqslant i < n$, collapses into

(10) 

with $\lambda^* = \lambda_1 + \cdots + \lambda_n$.

The types $\mathfrak{t}'$ and $\mathfrak{t}''$ are "equivalent", and this means that $\mathbb{P}(\mathfrak{t}) = \mathbb{P}(\mathfrak{t}')$, where $\mathbb{P}(\mathfrak{t})$ is the set of prime polynomials $g \in \mathcal{O}_v[x]$ which are divisible by $\mathfrak{t}$ [10, Thm. 3.7].

The existence of the non-optimised tree is useful in many situations. Let us see an example.

Lemma 5.8. *Let $\mathfrak{t}, \mathfrak{t}' \in \mathfrak{T}^{\mathrm{nop}}$. If $\mathfrak{t}$ is a truncation of $\mathfrak{t}'$, then $\mathbb{P}(\mathfrak{t}) \supset \mathbb{P}(\mathfrak{t}')$. If neither of these types is a truncation of the other, then $\mathbb{P}(\mathfrak{t}) \cap \mathbb{P}(\mathfrak{t}') = \varnothing$.*

Proof. The first statement is an immediate consequence of Theorem 5.6.

The second statement is obvious if $\mathfrak{t}$ and $\mathfrak{t}'$ have different root nodes, because for all $F \in \mathbb{P}(\mathfrak{t})$, the reduction $\overline{F}$ modulo $\mathfrak{m}$ is a power of the monic irreducible polynomial ψ_0 corresponding to the root node of $\mathfrak{t}$.

Suppose that $\mathfrak{t}, \mathfrak{t}'$ have the same root node and let $\mathfrak{t}_0$ be the greatest common node in the paths joining $\mathfrak{t}, \mathfrak{t}'$ with their root node. By the first statement we may assume that $\mathfrak{t}$ and $\mathfrak{t}'$ are branches of $\mathfrak{t}_0$, in other words, that $\mathfrak{t}_0$ is the previous node of both $\mathfrak{t}$ an $\mathfrak{t}'$. By the coherence of $\mathfrak{T}^{\mathrm{nop}}$ we have

$$\mathfrak{t} = (\mathfrak{t}_0; (\phi, \lambda, \psi)), \qquad \mathfrak{t}' = (\mathfrak{t}_0; (\phi, \lambda', \psi')),$$

where either $\lambda \neq \lambda'$ or $\lambda = \lambda', \psi \neq \psi'$.

Let r be the order of $\mathfrak{t}_0$ and v_r its attached valuation. Now, for any $F \in \mathbb{P}(\mathfrak{t})$, $F' \in \mathbb{P}(\mathfrak{t}')$, Theorem 5.6 shows that $\mathrm{N}_{v_r,\phi}(F)$ and $\mathrm{N}_{v_r,\phi}(F')$ are one-sided of slopes $-\lambda$ and $-\lambda'$ respectively. Hence, $\lambda \neq \lambda'$ implies $F \neq F'$. On the other hand, if $\lambda = \lambda'$ then $\mathrm{R}_{\mathfrak{t}_0,\phi,\lambda}(F) = \psi^a$ and $\mathrm{R}_{\mathfrak{t}_0,\phi,\lambda}(F') = (\psi')^{a'}$ and this implies $F \neq F'$, because $\psi \neq \psi'$. □

This result may be false for arbitrary incoherent trees. However, Lemma 5.8 is valid for the optimised tree $\mathfrak{T}$ of OM representations of the prime factors of f.

Proposition 5.9. *Let $\mathfrak{t}, \mathfrak{t}' \in \mathfrak{T}$ be two nodes such that neither of them is a truncation of the other. Then $\mathbb{P}(\mathfrak{t}) \cap \mathbb{P}(\mathfrak{t}') = \varnothing$. In particular, $\mathcal{P}_\mathfrak{t} \cap \mathcal{P}_{\mathfrak{t}'} = \varnothing$.*

Proof. Clearly, the nodes $\mathfrak{t}, \mathfrak{t}'$ are equivalent to two nodes of the non-optimised tree, neither of them being a truncation of the other. Thus, the statement is an immediate consequence of Lemma 5.8.

The final statement is a consequence of $\mathcal{P}_\mathfrak{t} = \{\mathfrak{p} \in \mathcal{P} : F_\mathfrak{p} \in \mathbb{P}(\mathfrak{t})\}$. □

Consider the chain of refinements that take place between (9) and (10). During each refinement that provokes branching of a type, the intermediate ϕ and λ values are stored.

Let $\mathtt{t}_{\mathfrak{p}}, \mathtt{t}_{\mathfrak{q}} \in \mathfrak{T}$ be two leaves attached to prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ with index of coincidence $i(\mathfrak{p},\mathfrak{q}) = \ell$. Then suppose that at level ℓ, each type has a list of stored refinements,

$$\begin{aligned} \mathrm{Ref}_\ell(\mathtt{t}_{\mathfrak{p}}) &= \left[(\phi_{(1)}^{\mathtt{t}_{\mathfrak{p}}}, \lambda_{(1)}^{\mathtt{t}_{\mathfrak{p}}}, \psi_{(1)}^{\mathtt{t}_{\mathfrak{p}}}), \ldots, (\phi_{(k)}^{\mathtt{t}_{\mathfrak{p}}}, \lambda_{(k)}^{\mathtt{t}_{\mathfrak{p}}}, \psi_{(k)}^{\mathtt{t}_{\mathfrak{p}}})\right], \\ \mathrm{Ref}_\ell(\mathtt{t}_{\mathfrak{q}}) &= \left[(\phi_{(1)}^{\mathtt{t}_{\mathfrak{q}}}, \lambda_{(1)}^{\mathtt{t}_{\mathfrak{q}}}, \psi_{(1)}^{\mathtt{t}_{\mathfrak{q}}}), \ldots, (\phi_{(k')}^{\mathtt{t}_{\mathfrak{q}}}, \lambda_{(k')}^{\mathtt{t}_{\mathfrak{q}}}, \psi_{(k')}^{\mathtt{t}_{\mathfrak{q}}})\right]. \end{aligned} \tag{11}$$

This allows us to extend the index of coincidence to a more precise indicator.

Definition 5.10. *The* minor index of coincidence $\hat{\imath}(\mathfrak{p},\mathfrak{q})$ *for two leaves* $\mathtt{t}_{\mathfrak{p}}, \mathtt{t}_{\mathfrak{q}} \in \mathfrak{T}$*, is the least index* ℓ'*, such that for the refinement lists given in* (11)*,*

$$(\phi_{(\ell')}^{\mathtt{t}_{\mathfrak{p}}}, \lambda_{(\ell')}^{\mathtt{t}_{\mathfrak{p}}}, \psi_{(\ell')}^{\mathtt{t}_{\mathfrak{p}}}) \neq (\phi_{(\ell')}^{\mathtt{t}_{\mathfrak{q}}}, \lambda_{(\ell')}^{\mathtt{t}_{\mathfrak{q}}}, \psi_{(\ell')}^{\mathtt{t}_{\mathfrak{q}}}).$$

We also define the extended index of coincidence *of two types as,*

$$I(\mathfrak{p},\mathfrak{q}) := [i(\mathfrak{p},\mathfrak{q}), \hat{\imath}(\mathfrak{p},\mathfrak{q})].$$

These extended indices of coincidence are ordered lexicographically.

Definition 5.11. *Let* $\mathtt{t}_{\mathfrak{p}}, \mathtt{t}_{\mathfrak{q}} \in \mathfrak{T}$ *be two leaves with index of coincidence* $i(\mathfrak{p},\mathfrak{q}) = \ell$ *and let the list of refinements of each type at level* ℓ *be as in* (11)*.*

1. *The* greatest common ϕ-polynomial *of the prime ideals* $\mathfrak{p},\mathfrak{q}$ *is* $\phi(\mathfrak{p},\mathfrak{q}) = \phi_{(j)}^{\mathtt{t}_{\mathfrak{p}}} = \phi_{(j)}^{\mathtt{t}_{\mathfrak{q}}}$*, with* j *maximal.*
2. *The (non-optimised)* hidden slopes *of the prime ideals* $\mathfrak{p},\mathfrak{q}$ *are* $(\lambda_{\mathfrak{p}}^{\mathfrak{q}})^{\mathrm{nop}} = \lambda_{(j)}^{\mathtt{t}_{\mathfrak{p}}}$ *and* $(\lambda_{\mathfrak{q}}^{\mathfrak{p}})^{\mathrm{nop}} = \lambda_{(j)}^{\mathtt{t}_{\mathfrak{q}}}$*, for this maximal value of* j*.*
3. *The (opimised) hidden slopes of the prime ideals* $\mathfrak{p},\mathfrak{q}$ *are* $\lambda_{\mathfrak{p}}^{\mathfrak{q}} = \lambda_{(1)}^{\mathtt{t}_{\mathfrak{p}}} + \cdots + \lambda_{(j)}^{\mathtt{t}_{\mathfrak{p}}}$ *and* $\lambda_{\mathfrak{q}}^{\mathfrak{p}} = \lambda_{(1)}^{\mathtt{t}_{\mathfrak{q}}} + \cdots + \lambda_{(j)}^{\mathtt{t}_{\mathfrak{q}}}$*, for the same maximal value of* j*.*

Remark 5.12. (1) By (10) $\lambda_{\ell,\mathfrak{p}} = \sum_{i=1}^{k} \lambda_{(i)}^{\mathtt{t}_{\mathfrak{p}}}$. In particular $\lambda_{\ell,\mathfrak{p}} \geqslant \lambda_{\mathfrak{p}}^{\mathfrak{q}}$, for all $\mathfrak{q} \in \mathcal{P}$ with $i(\mathfrak{p},\mathfrak{q}) = \ell$.

(2) Proposition 2.3 is easily deduced from Theorem 5.7. Since this theorem is valid for arbitrary types, it is clear that the formulas in Proposition 2.3 are valid for the ϕ-polynomials of the non-optimised tree just by replacing the optimised hidden slopes with the non-optimised ones.

5.3. **Optimal polynomials as products of ϕ-polynomials.** Let $S \subseteq \mathcal{P}$ be a subset of prime ideals. Let $\mathfrak{T}_S$ be the tree of OM representations of the prime ideals $\mathfrak{p} \in S$ computed by the Montes algorithm. We keep the content of Section 2 concerning the data attached to the different types $\mathtt{t}_{\mathfrak{p}}$ for $\mathfrak{p} \in S$. We recall that the polynomials $\phi_{\mathfrak{p}} \in \mathcal{O}[x]$ are concrete choices of Okutsu approximations to the prime factors $F_{\mathfrak{p}}$ of f.

The ϕ-polynomials for all the prime ideals generate a semigroup.

Definition 5.13. *Let* $S \subseteq \mathcal{P}$ *be a set of prime ideals. We denote by* $\Phi(S) \subset \mathcal{O}[x]$ *the multiplicative semigroup generated by*

$$\{\phi_{i,\mathfrak{p}} : \mathfrak{p} \in S,\ 0 \leqslant i \leqslant r_{\mathfrak{p}}\} \cup \bigcup_{\mathfrak{p} \in S} \mathrm{App}(\mathfrak{p}),$$

where $\mathrm{App}(\mathfrak{p}) = \{\phi \in \mathcal{O}[x]$ *monic of degree* $n_\mathfrak{p}$ *such that* $w_\mathfrak{p}(\phi(\theta)) \geqslant w_\mathfrak{p}(\phi_\mathfrak{p}(\theta))\}$.

We use $\Phi(\mathfrak{p})$ *to denote* $\Phi(\{\mathfrak{p}\})$.

We are interested in showing that we can restrict our search for polynomials of a given degree d with maximal $w_{S,I}$-value to those in the semigroup $\Phi(S)$.

Definition 5.14. *Let* $g \in \mathcal{O}[x]$. *The* degree adjusted $w_\mathfrak{p}$*-valuation of the element* $g(\theta) \in \mathcal{O}_L$ *is defined as*

$$\hat{w}_\mathfrak{p}(g(\theta)) := \frac{w_\mathfrak{p}(g(\theta))}{\deg g}.$$

Lemma 5.15. *Let* $\mathfrak{t}$ *be a node in the non-optimised tree* $\mathfrak{T}^{\mathrm{nop}}$ *and let* $g, h \in \mathcal{O}_v[x]$ *be two prime polynomials divisible by* $\mathfrak{t}$. *Then, for any prime ideal* $\mathfrak{p} \in \mathcal{P} \backslash \mathcal{P}_\mathfrak{t}$ *we have* $\hat{w}_\mathfrak{p}(g(\theta)) = \hat{w}_\mathfrak{p}(h(\theta))$.

Proof. If $\mathfrak{t}$ and $\mathfrak{t}_\mathfrak{p}$ have different root nodes, we have $w_\mathfrak{p}(g(\theta)) = 0 = w_\mathfrak{p}(h(\theta))$, because $\overline{F}_\mathfrak{p}$ is a power of $\psi_{0,\mathfrak{p}}$ and $\overline{g}$, $\overline{h}$ are powers of the root node of $\mathfrak{t}$.

If $\mathfrak{t}$ and $\mathfrak{t}_\mathfrak{p}$ have the same root node, let $\mathfrak{t}_0$ be the greatest common node in the paths of $\mathfrak{T}^{\mathrm{nop}}$ joining $\mathfrak{t}_\mathfrak{p}$ and $\mathfrak{t}$ with the root node. Since $\mathfrak{p} \notin \mathcal{P}_\mathfrak{t}$, the node $\mathfrak{t}_0$ cannot be equal to $\mathfrak{t}$. Since $\mathfrak{t}_\mathfrak{p}$ is a leaf of the tree, $\mathfrak{t}_0$ cannot be equal to $\mathfrak{t}_\mathfrak{p}$ either. The structure of the non-optimised tree is shown in Figure 6.

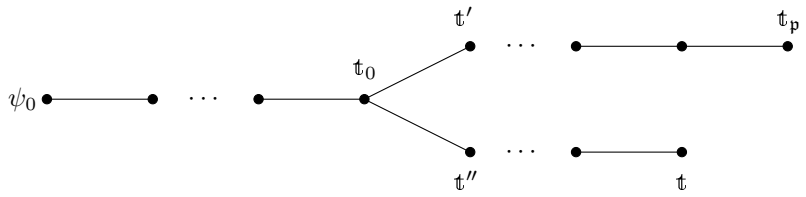


FIGURE 6. The node $\mathfrak{t}_0$ is the greatest common node of $\mathfrak{t}$ and $\mathfrak{t}_\mathfrak{p}$.

Let $\mathfrak{t}', \mathfrak{t}''$ be the nodes following $\mathfrak{t}_0$ in each of the two paths. Since the non-optimised tree is coherent, we have

$$\mathfrak{t}' = (\mathfrak{t}_0; (\phi, \lambda', \psi')), \qquad \mathfrak{t}'' = (\mathfrak{t}_0; (\phi, \lambda'', \psi'')),$$

with a common choice for the representative ϕ of $\mathfrak{t}_0$.

By Theorem 5.6, $\mathrm{N}_{v_{\mathfrak{t}_0},\phi}(g)$ and $\mathrm{N}_{v_{\mathfrak{t}_0},\phi}(h)$ are one-sided of slope $-\lambda''$. Proposition 5.9 shows that $\mathfrak{t}' \nmid g$, $\mathfrak{t}' \nmid h$. By Theorem 5.7, we have

$$\hat{w}_\mathfrak{p}(g(\theta)) = \frac{1}{\deg \phi} \cdot \frac{V_{r+1} + \mathrm{Min}\{\lambda', \lambda''\}}{e_1 \cdots e_r} = \hat{w}_\mathfrak{p}(h(\theta)),$$

where r is the order of $\mathfrak{t}_0$. □

The next result is the main aim of this section.

Proposition 5.16. *Let* $S \subseteq \mathcal{P}$ *be a set of prime ideals. For any* $h \in \mathcal{O}_v[x]$ *monic of degree* $0 \leqslant d < n$, *there exists* $\phi \in \Phi(\mathcal{P})$ *also of degree* d *such that,*

$$w_\mathfrak{p}(\phi(\theta)) \geqslant w_\mathfrak{p}(h(\theta)), \qquad \forall\ \mathfrak{p} \in S. \tag{12}$$

Proof. The proof will proceed by induction on the degree d of the polynomial. We will work in steps, in each one reducing the space in which we need to consider h.

If $d = 0$, then $\phi = h = 1 \in \Phi(S)$.

Claim. *It is sufficient to check* (12) *for* h *a prime polynomial.*

Let $h = h_1 h_2$, with $h_1, h_2 \in \mathcal{O}_v[x]$ monic of degree $d_1, d_2 > 0$ respectively.

By the induction hypothesis, there exist $\phi_i \in \Phi(S)$ of degree d_i such that,

$$w_{\mathfrak{p}}\left(\phi_i(\theta)\right) \geqslant w_{\mathfrak{p}}\left(h_i(\theta)\right), \qquad \forall\ \mathfrak{p} \in S,$$

for $i = 1, 2$. Then, $\phi = \phi_1 \phi_2 \in \Phi(S)$ clearly satisfies (12). This proves the claim.

Now, assume that h is a prime polynomial. If $\gcd(\overline{f}, \overline{h}) = 1$, then $w_{\mathfrak{p}}\left(h(\theta)\right) = 0$ for all $\mathfrak{p} \in S$. Thus, (12) is obviously satisfied.

Therefore, we can assume that $\overline{h} = \psi_0^b$, $b \in \mathbb{N}$, for $\psi_0 \in \mathbb{F}[y]$ a prime factor of $\overline{f}$.

By hypothesis, the root node ψ_0 (thought of as a type of order zero) divides h. Let $\mathfrak{t}$ be the highest order node in the non-optimised tree $\mathfrak{T}_S^{\mathrm{nop}}$ such that $\mathfrak{t} \mid h$, and let i be the order of $\mathfrak{t}$. We distinguish two cases according to $\mathfrak{t}$ being a leaf or not.

Case 1. $\mathfrak{t}$ is a leaf.

In this case, $S_{\mathfrak{t}} = \{\mathfrak{p}_0\}$ contains only one prime ideal. The ϕ-polynomial in the last level of $\mathfrak{t}$ is an Okutsu approximation $\phi_{\mathfrak{p}_0}$ to $F_{\mathfrak{p}_0}$. Since $\mathfrak{t} \mid h$, Theorem 5.5 shows that $\deg h = \ell \cdot \deg \phi_{\mathfrak{p}_0} = \ell \cdot n_{\mathfrak{p}_0}$ for some positive integer ℓ, and $v_{\mathfrak{p}_0}\left(h(\theta)\right) > v_{\mathfrak{p}_0}\left(\phi_{\mathfrak{p}_0}(\theta)\right)$.

Let us consider $\phi_0 \in \mathrm{App}(\mathfrak{p}_0)$ and close enough to $F_{\mathfrak{p}_0}$ so that

$$w_{\mathfrak{p}_0}\left(\phi_0(\theta)\right) \geqslant w_{\mathfrak{p}_0}\left(h(\theta)\right)/\ell,$$

and take $\phi = \phi_0^{\ell} \in \Phi(S)$. By construction, $w_{\mathfrak{p}_0}\left(\phi(\theta)\right) \geqslant w_{\mathfrak{p}_0}\left(h(\theta)\right)$. On the other hand, for any $\mathfrak{p} \in S$, $\mathfrak{p} \neq \mathfrak{p}_0$, we clearly have $\hat{w}_{\mathfrak{p}}\left(\phi(\theta)\right) = \hat{w}_{\mathfrak{p}}\left(\phi_0(\theta)\right)$ and Lemma 5.15 shows that $\hat{w}_{\mathfrak{p}}\left(\phi_0(\theta)\right) = \hat{w}_{\mathfrak{p}}\left(h(\theta)\right)$. Since $\deg(\phi) = \deg(h)$ we deduce that $w_{\mathfrak{p}}\left(\phi(\theta)\right) = w_{\mathfrak{p}}\left(h(\theta)\right)$. This proves (12).

Case 2. $\mathfrak{t}$ is not a leaf.

For a certain choice $\phi_{\mathfrak{t}}$ of a representative of $\mathfrak{t}$, the node $\mathfrak{t}$ has several branches in the non-optimised tree, of the form

$$\mathfrak{t}_{\lambda,\psi} = (\mathfrak{t}; (\phi_{\mathfrak{t}}, \lambda, \psi)).$$

By the maximality of $\mathfrak{t}$, we have $\mathfrak{t}_{\lambda,\psi} \nmid h$ for all these branch nodes. Let $\lambda_{\max}$ be the greatest slope (in absolute size) of these branches and let $\mathfrak{t}_{\max}$ be any branch node of $\mathfrak{t}$ with slope $\lambda_{\max}$.

Since $\mathfrak{t} \mid h$, Theorem 5.5 shows that $\mathrm{N}_{v_{\mathfrak{t}},\phi_{\mathfrak{t}}}(h)$ is one-sided of slope $-\lambda_h$ and $\deg(h) = \ell \deg(\phi_{\mathfrak{t}})$, for certain positive $\lambda_h \in \mathbb{Q}$, $\ell \in \mathbb{Z}$.

If for some $\mathfrak{p}_0 \in S_{\mathfrak{t}}$ we take $\phi_{j,\mathfrak{p}_0}$ satisfying:

$$\deg(\phi_{j,\mathfrak{p}_0}) = \deg(\phi_{\mathfrak{t}}), \qquad \mathfrak{t} \mid \phi_{j,\mathfrak{p}_0}, \tag{13}$$

then Lemma 5.15 shows that $\hat{w}_{\mathfrak{p}}\left(h(\theta)\right) = \hat{w}_{\mathfrak{p}}\left(\phi_{j,\mathfrak{p}_0}(\theta)\right)$ for all $\mathfrak{p} \notin S_{\mathfrak{t}}$. As in Case 1, for $\phi = \phi_{j,\mathfrak{p}_0}^{\ell} \in \Phi(S)$ this implies $w_{\mathfrak{p}}\left(h(\theta)\right) = w_{\mathfrak{p}}\left(\phi(\theta)\right)$ for all $\mathfrak{p} \notin S_{\mathfrak{t}}$. Therefore, we need only to find some $\phi_{j,\mathfrak{p}_0}$ satisfying (13) and $w_{\mathfrak{p}}\left(\phi_{j,\mathfrak{p}_0}(\theta)\right) \geqslant \ell^{-1} w_{\mathfrak{p}}\left(h(\theta)\right)$ for all $\mathfrak{p} \in S_{\mathfrak{t}}$. Then we shall have (12).

Let $\mathfrak{t}'$ be any node of the optimised tree which has been derived from $\mathfrak{t}_{\max}$ by a series of refinement steps as indicated in (9) and (10).

Let $(\phi_0, \lambda_0, \psi_0)$ be the last level of $\mathfrak{t}'$ in the non-optimised tree. As explained in Section 5.2 the last level of $\mathfrak{t}'$ as a type from the optimised tree will be $(\phi_0, \lambda_0^*, \psi_0)$, where λ_0^* is the sum of all the slopes of all bad levels between $\mathfrak{t}'$ and its previous node in the optimised tree.

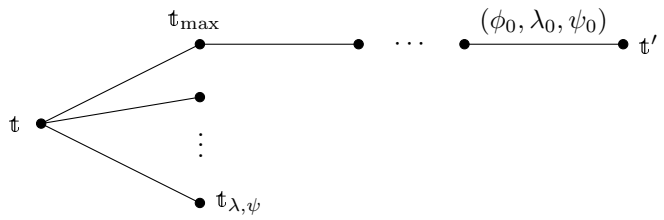


FIGURE 7. The node $\mathfrak{t}'$ corresponds to a node of the optimised tree.

Thus, $\phi_0 = \phi_{j,\mathfrak{p}_0}$ for all $\mathfrak{p}_0 \in S_{\mathfrak{t}'}$, where j is the order of $\mathfrak{t}'$ as a type of the optimised tree. Clearly, $\phi_{j,\mathfrak{p}_0}$ satisfies (13); let us compare $w_{\mathfrak{p}}\left(\phi_{j,\mathfrak{p}_0}(\theta)\right)$ and $w_{\mathfrak{p}}\left(h(\theta)\right)$ for $\mathfrak{p} \in S_{\mathfrak{t}}$. Take $\mathfrak{p} \in S_{\mathfrak{t}}$ and let $\mathfrak{t}_{\lambda,\psi}$ be the unique branch of $\mathfrak{t}$ such that $\mathfrak{t}_{\lambda,\psi} \mid F_{\mathfrak{p}}$. By Theorem 5.7,

$$\ell^{-1} w_{\mathfrak{p}}\left(h(\theta)\right) = \frac{V_{i+1} + \operatorname{Min}\{\lambda_h, \lambda\}}{e_1 \cdots e_i} \leqslant \frac{V_{i+1} + \lambda}{e_1 \cdots e_i}.$$

Thus, we need only to show that

$$w_{\mathfrak{p}}\left(\phi_0(\theta)\right) \geqslant \frac{V_{i+1} + \lambda}{e_1 \cdots e_i}.$$

Suppose that $\mathfrak{t}_{\max}$ gives rise to a node of the optimised tree. In this case, we have $\mathfrak{t}_{\max} = \mathfrak{t}'$ and $\phi_0 = \phi_{\mathfrak{t}}$. By Theorem 5.5, $w_{\mathfrak{p}}\left(\phi_0(\theta)\right) = (V_{i+1} + \lambda)/(e_1 \cdots e_i)$. From now on we assume that $\mathfrak{t}_{\max} \neq \mathfrak{t}'$.

If $\mathfrak{t}_{\lambda,\psi} \neq \mathfrak{t}_{\max}$, then $\mathfrak{t} \mid \phi_0$, $\mathfrak{t}_{\lambda,\psi} \nmid \phi_0$ by Proposition 5.9; hence Theorem 5.7 shows that

$$w_{\mathfrak{p}}\left(\phi_0(\theta)\right) = \frac{V_{i+1} + \operatorname{Min}\{\lambda, \lambda_{\max}\}}{e_1 \cdots e_i} = \frac{V_{i+1} + \lambda}{e_1 \cdots e_i}.$$

Finally, suppose that $\mathfrak{t}_{\lambda,\psi} = \mathfrak{t}_{\max}$. The order of $\mathfrak{t}'$ as a type of the non-optimised tree is $\geqslant i+2$. By Proposition 2.3 applied to the non-optimised tree (see Remark 5.12) we have

$$w_{\mathfrak{p}}\left(\phi_0(\theta)\right) > \frac{V_{i+2,\mathfrak{p}}}{e_1 \cdots e_i e_{i+1,\mathfrak{p}}} = \frac{e_{i+1,\mathfrak{p}} f_{i+1,\mathfrak{p}} (e_{i+1,\mathfrak{p}} V_{i+1} + h_{i+1,\mathfrak{p}})}{e_1 \cdots e_i e_{i+1,\mathfrak{p}}} = \frac{V_{i+1} + \lambda}{e_1 \cdots e_i},$$

because $e_{i+1,\mathfrak{p}} = f_{i+1,\mathfrak{p}} = 1$ and $\lambda = h_{i+1,\mathfrak{p}}$. Thus, in all cases we obtain the desired inequality. □

5.4. **Optimal polynomials as products of numerators of Okutsu bases.** By Proposition 2.3, for any $\mathfrak{p} \in S$ we have

$$(14)\quad \hat{w}_{\mathfrak{p}}\left(\phi_{i,\mathfrak{p}}(\theta)\right) = \frac{1}{m_i} \frac{V_i + \lambda_i}{e_1 \cdots e_{i-1}} = \frac{1}{m_{i+1}} \frac{V_{i+1}}{e_1 \cdots e_i} < \hat{w}_{\mathfrak{p}}\left(\phi_{i+1,\mathfrak{p}}(\theta)\right), \quad 1 \leqslant i \leqslant r_{\mathfrak{p}}.$$

Let us analyse how closely we can replicate this inequality (14) for cross valuations, that is to say when the ϕ-polynomial belongs to a different prime to that of the valuation. The next results follow closely form Proposition 2.3 too.

Lemma 5.17. *Let $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$ be two different prime ideals with index of coincidence $\ell = i(\mathfrak{p}, \mathfrak{q})$. Then:*

(1) $\hat{w}_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right) < \hat{w}_{\mathfrak{p}}\left(\phi_{i+1,\mathfrak{q}}(\theta)\right), \quad 1 \leqslant i < \ell,$
(2) $\hat{w}_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right) = \hat{w}_{\mathfrak{p}}\left(\phi_{i+1,\mathfrak{q}}(\theta)\right), \quad \ell < i \leqslant r_{\mathfrak{p}}.$

It is easy to find examples where

$$\hat{w}_{\mathfrak{p}}\left(\phi_{\ell,\mathfrak{q}}(\theta)\right) > \hat{w}_{\mathfrak{p}}\left(\phi_{\ell+1,\mathfrak{q}}(\theta)\right). \tag{15}$$

This pathology occurs when $\phi_{\ell,\mathfrak{q}} = \phi(\mathfrak{p},\mathfrak{q})$ and $\lambda_{\mathfrak{p}}^{\mathfrak{q}}$ is much larger than $\lambda_{\mathfrak{q}}^{\mathfrak{p}}$ (see Proposition 2.3). Hence, it is also easy to find specific conditions that avoid (15).

Lemma 5.18. *Let $\mathfrak{p},\mathfrak{q} \in \mathcal{P}$ be two different prime ideals with $\ell = i(\mathfrak{p},\mathfrak{q}) > 0$, chosen so that $\lambda_{\mathfrak{q}}^{\mathfrak{p}} \geqslant \lambda_{\mathfrak{p}}^{\mathfrak{q}}$. Then,*

$$\hat{w}_{\mathfrak{p}}\left(\phi_{\ell,\mathfrak{q}}(\theta)\right) = \hat{w}_{\mathfrak{p}}\left(\phi_{\ell+1,\mathfrak{q}}(\theta)\right). \tag{16}$$

In particular, every numerator $g_{i,\mathfrak{q}}$ of degree i of the Okutsu $\mathfrak{q}$-basis has maximal $\mathfrak{p}$-valuation amongst all polynomials $\phi \in \Phi(\mathfrak{q})$ of degree i.

Proof. By the hypothesis, $\operatorname{Min}\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\} = \lambda_{\mathfrak{p}}^{\mathfrak{q}}$ and Proposition 2.3 gives (16). Therefore, Lemma 5.17 and (16) show that the $\mathfrak{p}$-valuations of the polynomials $\phi_{i,\mathfrak{q}}$ increase with their degree up to index ℓ and then remain equal. As such, we will always have a maximal valuation by taking higher degree ϕ-polynomials, rather than products of smaller degree ones. □

Using the extended index of coincidence presented in Definition 5.10, the following Lemma gives us a link between the relative similarity of prime ideals and their respective cross-valuations in certain cases.

Lemma 5.19. *For a prime ideal $\mathfrak{q} \in \mathcal{P}$, let $\mathfrak{p},\mathfrak{l} \in \mathcal{P}\setminus\{\mathfrak{q}\}$ be two prime ideals such that either $\mathfrak{l} = \mathfrak{p}$ or they satisfy:*

1. *$I(\mathfrak{l},\mathfrak{q}) \geqslant I(\mathfrak{p},\mathfrak{q})$, and*
2. *$\lambda_{\mathfrak{l}}^{\mathfrak{q}} \geqslant \lambda_{\mathfrak{p}}^{\mathfrak{q}}$ if $I(\mathfrak{l},\mathfrak{q}) = I(\mathfrak{p},\mathfrak{q})$.*

Then, for $\ell = i(\mathfrak{l},\mathfrak{q})$ and $m_\ell = m_{\ell,\mathfrak{q}} = m_{\ell,\mathfrak{l}}$, we have

$$w_{\mathfrak{p}}\left(\phi_{\ell,\mathfrak{l}}^{m_{i,\mathfrak{q}}/m_\ell}(\theta)\right) \geqslant w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right), \qquad \ell \leqslant i \leqslant r_{\mathfrak{q}}+1.$$

Proof. We may consider four cases depending on the relationship between the three prime ideals $\mathfrak{p}$, $\mathfrak{q}$, and $\mathfrak{l}$.

Case 1. $i(\mathfrak{l},\mathfrak{q}) > i(\mathfrak{p},\mathfrak{q})$. In this case, $k := i(\mathfrak{p},\mathfrak{l}) = i(\mathfrak{p},\mathfrak{q}) < \ell$ and $\lambda_{\mathfrak{q}}^{\mathfrak{p}} = \lambda_{\mathfrak{l}}^{\mathfrak{p}}$, $\lambda_{\mathfrak{p}}^{\mathfrak{q}} = \lambda_{\mathfrak{p}}^{\mathfrak{l}}$. Therefore, for $\ell \leqslant i \leqslant r_{\mathfrak{q}}+1$, Proposition 2.3 shows that

$$\begin{aligned} w_{\mathfrak{p}}\left(\phi_{\ell,\mathfrak{l}}^{m_{i,\mathfrak{q}}/m_\ell}(\theta)\right) &= \frac{m_{i,\mathfrak{q}}}{m_\ell}\frac{m_\ell}{m_k}\frac{V_k + \operatorname{Min}\left\{\lambda_{\mathfrak{p}}^{\mathfrak{l}}, \lambda_{\mathfrak{l}}^{\mathfrak{p}}\right\}}{e_1\cdots e_{k-1}} \\ &= \frac{m_{i,\mathfrak{q}}}{m_k}\frac{V_k + \operatorname{Min}\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1\cdots e_{k-1}} = w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right). \end{aligned} \tag{17}$$

Case 2. $i(\mathfrak{l},\mathfrak{q}) = i(\mathfrak{p},\mathfrak{q})$ and either $\mathfrak{l} = \mathfrak{p}$ or $i(\mathfrak{p},\mathfrak{l}) > \ell$. We have

$$w_{\mathfrak{p}}\left(\phi_{\ell,\mathfrak{l}}^{m_{i,\mathfrak{q}}/m_\ell}(\theta)\right) = \frac{m_{i,\mathfrak{q}}}{m_\ell}\frac{V_\ell + \lambda_{\ell,\mathfrak{p}}}{e_1\cdots e_{\ell-1}}$$

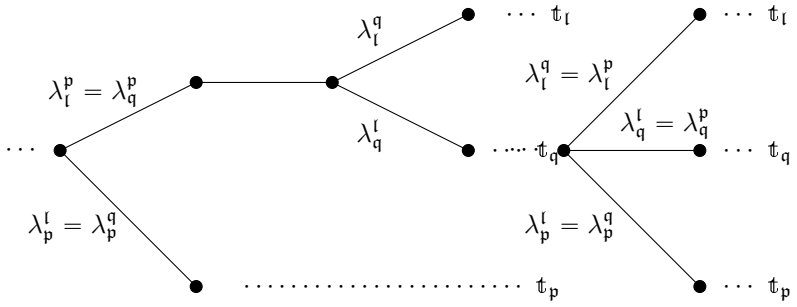
by Proposition 2.3. On the other hand,

$$w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right) = \begin{cases} \dfrac{V_\ell + \lambda_{\mathfrak{p}}^{\mathfrak{q}}}{e_1\cdots e_{\ell-1}}, & \text{if } i = \ell \text{ and } \phi_{\ell,\mathfrak{q}} = \phi(\mathfrak{p},\mathfrak{q}), \\ \dfrac{m_{i,\mathfrak{q}}}{m_\ell}\dfrac{V_\ell + \operatorname{Min}\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}}{e_1\cdots e_{\ell-1}}, & \text{otherwise.} \end{cases} \tag{18}$$

By the first item of Remark 5.12, we have $\lambda_{\mathfrak{p}}^{\mathfrak{q}} \leqslant \lambda_{\ell,\mathfrak{p}}$, so that $w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right) \leqslant w_{\mathfrak{p}}\left(\phi_{\ell,\mathfrak{l}}^{m_{i,\mathfrak{q}}/m_\ell}(\theta)\right)$ in both cases.

Case 3. $i(\mathfrak{l},\mathfrak{q}) = i(\mathfrak{p},\mathfrak{q}) = i(\mathfrak{p},\mathfrak{l})$, and $I(\mathfrak{l},\mathfrak{q}) > I(\mathfrak{p},\mathfrak{q})$. In the non-optimised tree, we find the situation described in Figure 8 (a), where we have written the optimised hidden slopes instead of the non-optimised ones.

We necessarily have $\phi_{\ell,\mathfrak{q}} \neq \phi(\mathfrak{p},\mathfrak{q}) = \phi(\mathfrak{p},\mathfrak{l}) \neq \phi_{\ell,\mathfrak{l}}$, and $\lambda_{\mathfrak{p}}^{\mathfrak{l}} = \lambda_{\mathfrak{p}}^{\mathfrak{q}}$, $\lambda_{\mathfrak{q}}^{\mathfrak{p}} = \lambda_{\mathfrak{l}}^{\mathfrak{p}}$. Therefore, the equations of (17) (where $k = \ell$ now) are again a consequence of Proposition 2.3, for all $\ell \leqslant i \leqslant r_{\mathfrak{q}} + 1$.



(a) $I(\mathfrak{l},\mathfrak{q}) > I(\mathfrak{l},\mathfrak{p})$. (b) $I(\mathfrak{l},\mathfrak{q}) = I(\mathfrak{l},\mathfrak{p})$.

FIGURE 8. Relative positions of $\mathfrak{t}_{\mathfrak{l}}$, $\mathfrak{t}_{\mathfrak{q}}$, and $\mathfrak{t}_{\mathfrak{p}}$ in the non-optimised tree when $i(\mathfrak{l},\mathfrak{q}) = i(\mathfrak{p},\mathfrak{q}) = i(\mathfrak{p},\mathfrak{l})$.

Case 4. $\mathfrak{p} \neq \mathfrak{l}$, $i(\mathfrak{l},\mathfrak{q}) = i(\mathfrak{p},\mathfrak{q}) = i(\mathfrak{p},\mathfrak{l})$, and $I(\mathfrak{l},\mathfrak{q}) = I(\mathfrak{p},\mathfrak{q})$. In the non-optimised tree, we find the situation described in Figure 8 (b). We have $\phi(\mathfrak{p},\mathfrak{q}) = \phi(\mathfrak{l},\mathfrak{q}) = \phi(\mathfrak{p},\mathfrak{l})$. By our assumptions, $\lambda_{\mathfrak{p}}^{\mathfrak{l}} \leqslant \lambda_{\mathfrak{l}}^{\mathfrak{p}}$ and Proposition 2.3 shows that:

$$w_{\mathfrak{p}}\left(\phi_{\ell,\mathfrak{l}}^{m_{i,\mathfrak{q}}/m_\ell}(\theta)\right) = \frac{m_{i,\mathfrak{q}}}{m_\ell}\frac{V_\ell + \lambda_{\mathfrak{p}}^{\mathfrak{l}}}{e_1\cdots e_{\ell-1}},$$

whereas $w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right)$ is given by (18). Since $\lambda_{\mathfrak{p}}^{\mathfrak{q}} = \lambda_{\mathfrak{p}}^{\mathfrak{l}}$, we get $w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right) \leqslant w_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}^{m_{i,\mathfrak{q}}/m_\ell}(\theta)\right)$ as desired. □

Definition 5.20. *Let $g = \prod_{\mathfrak{p}} \varphi_{\mathfrak{p}} \in \Phi(S)$. The* disorder *of g is calculated as* $\mathrm{D}(g) = \sum_{\mathfrak{p}\in S} \max\{\deg(\varphi_{\mathfrak{p}}) - n_{\mathfrak{p}}, 0\}$.

Definition 5.21. *A polynomial $\varphi_{\mathfrak{p}} = \phi_{0,\mathfrak{p}}^{a_0}\phi_{1,\mathfrak{p}}^{a_1}\cdots\phi_{r_{\mathfrak{p}},\mathfrak{p}}^{a_{r_{\mathfrak{p}}}}\phi_{\mathfrak{p}}^{a_{r_{\mathfrak{p}}+1}} \in \Phi(\mathfrak{p})$ is said to be* canonical *if $0 \leqslant a_i < e_{i,\mathfrak{p}}f_{i,\mathfrak{p}}$ for all $0 \leqslant i \leqslant r_{\mathfrak{p}}$.*

The canonical polynomials $\varphi_{\mathfrak{p}} \in \Phi(\mathfrak{p})$ of degree $\deg(\varphi_{\mathfrak{p}}) \leqslant n_{\mathfrak{p}}$ coincide with the numerators of the Okutsu $\mathfrak{p}$-basis, and hence belong to $\mathrm{Ok}(\mathfrak{p})$ too.

Remark 5.22. For a given set of prime ideals $S \subseteq \mathcal{P}$, all of them with the same root node, it is always possible to choose a prime ideal $\mathfrak{p}_0 \in S$ such that $\lambda_{\mathfrak{p}_0}^{\mathfrak{p}} \leqslant \lambda_{\mathfrak{p}}^{\mathfrak{p}_0}$ for all $\mathfrak{p} \in S$.

To do so, begin at the root of the tree of types representing S and move up through the levels. When branching is encountered, take the branch that corresponds to the slope of least absolute value at that level. We continue in this way

until we reach a leaf node, which will correspond to a prime $\mathfrak{p}_0$ with the desired properties.

Proposition 5.23. *Let $S \subseteq \mathcal{P}$ be a set of prime ideals and consider $\phi \in \Phi(S)$ monic of degree $0 \leqslant d \leqslant n_S$. For appropriate choices of the Okutsu approximations $\phi_{\mathfrak{p}}$, the set $\mathrm{Ok}(S)$ contains a polynomial g of degree d such that,*

$$w_{\mathfrak{p}}\left(g(\theta)\right) \geqslant w_{\mathfrak{p}}\left(\phi(\theta)\right), \qquad \forall\ \mathfrak{p} \in S.$$

Proof. Consider $\phi = \prod_{\mathfrak{p}\in S} \varphi_{\mathfrak{p}}$ the separation of the polynomial ϕ into its $\mathfrak{p}$-parts $\varphi_{\mathfrak{p}}$ for each $\mathfrak{p} \in S$. Then, let $S_0 = \{\mathfrak{p} \in S : \varphi_{\mathfrak{p}} \neq \phi_{\mathfrak{p}}\}$.

We will follow an iterative sequence of three steps to find a polynomial $g \in \mathrm{Ok}(S)$ that meets the requirements of the proposition. Throughout this process we will be modifying g, which is initially set to ϕ, via its individual $\mathfrak{p}$-parts:

(1) For all $\mathfrak{p} \in S_0$, make $\varphi_{\mathfrak{p}}$ canonical.
(2) If $D(g) = 0$, then for all $\mathfrak{p} \in S\backslash S_0$ we take $\varphi_{\mathfrak{p}} = \phi_{\mathfrak{p}}$ to be an Okutsu approximation to $F_{\mathfrak{p}}$ with $w_{\mathfrak{p}}\left(\phi_{\mathfrak{p}}(\theta)\right) \geqslant w_{\mathfrak{p}}\left(\phi(\theta)\right)$, and finish the iterative process.
(3) Fix some $\mathfrak{q} \in S_0$ with $\deg(\varphi_{\mathfrak{q}}) > n_{\mathfrak{q}}$ and then select $\mathfrak{l} \in S_0$, the "closest" prime ideal to $\mathfrak{q}$. Transfer all ϕ-polynomials in $\varphi_{\mathfrak{q}}$, except for a single $\phi_{\mathfrak{q}}$, to $\varphi_{\mathfrak{l}}$. Remove $\mathfrak{q}$ from S_0.

Below, we will show that at each step, the $\mathfrak{p}$-valuation of g does not decrease for all $\mathfrak{p} \in S_0$ and that the process will terminate in a polynomial g belonging to $\mathrm{Ok}(S)$ after a finite number of iterations. The inequality $w_{\mathfrak{p}}\left(g(\theta)\right) \geqslant w_{\mathfrak{p}}\left(\phi(\theta)\right)$ for the primes $\mathfrak{p} \in S\backslash S_0$ are a consequence of the choices in Step (2).

Step 1. We will make $\varphi_{\mathfrak{p}}$ canonical for each $\mathfrak{p} \in S_0$ in turn. Initially, we set $S' = S_0$. Take $\mathfrak{q} \in S'$ such that $\lambda_{\mathfrak{q}}^{\mathfrak{p}} \leqslant \lambda_{\mathfrak{p}}^{\mathfrak{q}}$ for all $\mathfrak{p} \in S'\backslash\{\mathfrak{q}\}$ and set $S' = S'\backslash\{\mathfrak{q}\}$.

Consider $\varphi_{\mathfrak{q}} = \prod_{i=0}^{r_{\mathfrak{q}}+1} \phi_{i,\mathfrak{q}}^{a_i}$. To make $\varphi_{\mathfrak{q}}$ canonical, we wish to have $a_i < e_{i,\mathfrak{q}} f_{i,\mathfrak{q}}$ for all $0 \leqslant i \leqslant r_{\mathfrak{q}}$. We will do this iteratively for $i = 0, 1, \ldots, r_{\mathfrak{q}}$.

Case 1. $a_i < e_{i,\mathfrak{q}} f_{i,\mathfrak{q}}$. In this case, we do nothing.

Case 2. $a_i \geqslant e_{i,\mathfrak{q}} f_{i,\mathfrak{q}}$ and $\hat{w}_{\mathfrak{p}}\left(\phi_{i,\mathfrak{q}}(\theta)\right) \leqslant \hat{w}_{\mathfrak{p}}\left(\phi_{i+1,\mathfrak{q}}(\theta)\right)$ for all $\mathfrak{p} \in S'$. We replace each $\phi_{i,\mathfrak{q}}^{e_{i,\mathfrak{q}} f_{i,\mathfrak{q}}}$ with a single $\phi_{i+1,\mathfrak{q}}$ in $\varphi_{\mathfrak{q}}$.

For all $\mathfrak{p} \in S_0$, the $\mathfrak{p}$-valuation of $\varphi_{\mathfrak{q}}$ will not decrease. In fact, for $\mathfrak{p} \in S'$ this is deduced from the condition of this case. For $\mathfrak{p} \in S_0\backslash S'$, this is a consequence of Lemmas 5.17 and 5.18.

Case 3. $a_i \geqslant e_{i,\mathfrak{q}} f_{i,\mathfrak{q}}$ and $\hat{w}_{\mathfrak{p}_0}\left(\phi_{i,\mathfrak{q}}(\theta)\right) > \hat{w}_{\mathfrak{p}_0}\left(\phi_{i+1,\mathfrak{q}}(\theta)\right)$ for some $\mathfrak{p}_0 \in S'$. In this case, we cannot simply exchange $\phi_{i,\mathfrak{q}}^{e_{i,\mathfrak{q}} f_{i,\mathfrak{q}}}$ for $\phi_{i+1,\mathfrak{q}}$ without lowering the $\mathfrak{p}_0$-valuation of $\varphi_{\mathfrak{q}}$.

Instead, take $\mathfrak{l} \in S'$ the prime ideal that is "closest" to $\mathfrak{q}$; that is, $I(\mathfrak{q}, \mathfrak{l}) \geqslant I(\mathfrak{q}, \mathfrak{p})$ for all $\mathfrak{p} \in S'$, and in the case of equality $\lambda_{\mathfrak{l}}^{\mathfrak{q}} \geqslant \lambda_{\mathfrak{p}}^{\mathfrak{q}}$. By Lemma 5.17 and the election of $\mathfrak{l}$ we must have $i(\mathfrak{q}, \mathfrak{l}) \geqslant i = i(\mathfrak{p}_0, \mathfrak{q})$.

We remove $\phi_{i,\mathfrak{q}}^{a_i - e_{i,\mathfrak{q}} f_{i,\mathfrak{q}} + 1}$ from $\varphi_{\mathfrak{q}}$ and insert $\phi_{i,\mathfrak{l}}^{a_i - e_{i,\mathfrak{q}} f_{i,\mathfrak{q}} + 1}$ into $\varphi_{\mathfrak{l}}$. If $i < \ell := i(\mathfrak{l}, \mathfrak{q})$ then $\phi_{i,\mathfrak{q}} = \phi_{i,\mathfrak{l}}$ and g has not changed (we have only redistributed its $\mathfrak{p}$-parts). If $i = \ell$, we must check that $w_{\mathfrak{p}}\left(\phi_{\ell,\mathfrak{l}}(\theta)\right) \geqslant w_{\mathfrak{p}}\left(\phi_{\ell,\mathfrak{q}}(\theta)\right)$ for all $\mathfrak{p} \in S_0$. For $\mathfrak{p} \in S'$ this is a consequence of Lemma 5.19.

By the maximality of $I(\mathfrak{l}, \mathfrak{q})$ amongst all prime ideals in S', the relative situation of $\mathbb{t}_{\mathfrak{q}}, \mathbb{t}_{\mathfrak{l}}, \mathbb{t}_{\mathfrak{p}_0}$ in the non-optimised tree is as indicated in Figure 9.

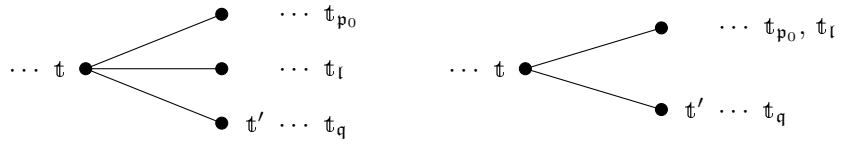


FIGURE 9. Relative position of $\mathfrak{t}_{\mathfrak{q}}, \mathfrak{t}_{\mathfrak{l}}, \mathfrak{t}_{\mathfrak{p}_0}$ in the non-optimised tree.

Also, by the remarks following (15), we have necessarily $\phi_{\ell,\mathfrak{q}} = \phi(\mathfrak{p}_0, \mathfrak{q})$; hence the node $\mathfrak{t}'$ in Figure 9 corresponds to a type in the optimised tree and $\lambda_{\ell,\mathfrak{q}} = \lambda_{\mathfrak{q}}^{\mathfrak{p}_0} = \lambda_{\mathfrak{q}}^{\mathfrak{l}}$. In particular, for any $\mathfrak{p} \in S$ with $i(\mathfrak{p}, \mathfrak{q}) = \ell$ we cannot have $I(\mathfrak{p}, \mathfrak{q}) > I(\mathfrak{l}, \mathfrak{q})$.

Now consider $\mathfrak{p} \in S_0 \backslash S'$. If $\mathfrak{p} \neq \mathfrak{q}$ and $I(\mathfrak{p}, \mathfrak{q}) \leqslant I(\mathfrak{l}, \mathfrak{q})$, Lemma 5.19 is also applicable and yields $w_{\mathfrak{p}}(\phi_{\ell,\mathfrak{l}}(\theta)) \geqslant w_{\mathfrak{p}}(\phi_{\ell,\mathfrak{q}}(\theta))$. If $I(\mathfrak{p}, \mathfrak{q}) > I(\mathfrak{l}, \mathfrak{q})$, we have necessarily $i(\mathfrak{p}, \mathfrak{q}) > \ell$, as we have just remarked above. This clearly implies $i(\mathfrak{p}, \mathfrak{l}) = \ell$.

In both cases, $\mathfrak{p} = \mathfrak{q}$ or $i(\mathfrak{p}, \mathfrak{q}) > i(\mathfrak{l}, \mathfrak{q}) = \ell$, Proposition 2.3 shows that:

$$w_{\mathfrak{p}}(\phi_{\ell,\mathfrak{q}}(\theta)) = \frac{V_\ell + \lambda_{\ell,\mathfrak{p}}}{e_1 \cdots e_{\ell-1}} = \frac{V_\ell + \lambda_{\ell,\mathfrak{q}}}{e_1 \cdots e_{\ell-1}},$$
$$w_{\mathfrak{p}}(\phi_{\ell,\mathfrak{l}}(\theta)) = \frac{V_\ell + \lambda_{\mathfrak{p}}^{\mathfrak{l}}}{e_1 \cdots e_{\ell-1}} = \frac{V_\ell + \lambda_{\mathfrak{q}}^{\mathfrak{l}}}{e_1 \cdots e_{\ell-1}}.$$

In the last equality, we used $\lambda_{\mathfrak{q}}^{\mathfrak{l}} = \operatorname{Min}\left\{\lambda_{\mathfrak{q}}^{\mathfrak{l}}, \lambda_{\mathfrak{l}}^{\mathfrak{q}}\right\}$, by the choice of $\mathfrak{q}$. Since $\lambda_{\ell,\mathfrak{q}} = \lambda_{\mathfrak{q}}^{\mathfrak{l}}$, we get $w_{\mathfrak{p}}(\phi_{\ell,\mathfrak{q}}(\theta)) = w_{\mathfrak{p}}(\phi_{\ell,\mathfrak{l}}(\theta))$ as desired.

We continue in this way until $\#S' = 0$.

Step 2. Having completed Step 1, all $\mathfrak{p}$-parts of g are canonical, so if $\mathrm{D}(g) = 0$, then $g \in \mathrm{Ok}(S)$, completing the process after considering adequate choices of the Okutsu approximations $\varphi_{\mathfrak{p}} = \phi_{\mathfrak{p}}$ for all $\mathfrak{p} \in S \backslash S_0$.

Step 3. If there exists $\mathfrak{q} \in S_0$ with $\deg \varphi_{\mathfrak{q}} > n_{\mathfrak{q}}$, we choose $\mathfrak{l} \in S_0$ such that $I(\mathfrak{q}, \mathfrak{l}) \geqslant I(\mathfrak{q}, \mathfrak{p})$ for all $\mathfrak{p} \in S_0 \backslash \{\mathfrak{q}\}$ and $\lambda_{\mathfrak{l}}^{\mathfrak{q}} \geqslant \lambda_{\mathfrak{p}}^{\mathfrak{q}}$ in the case of equality.

Having chosen $\mathfrak{q}$ and $\mathfrak{l}$, the transfer occurs as follows for each $0 \leqslant i \leqslant r_{\mathfrak{q}} + 1$:

$$\phi_{i,\mathfrak{q}} \longrightarrow \begin{cases} \phi_{i,\mathfrak{l}} & \text{if } i < \ell = i(\mathfrak{q}, \mathfrak{l}), \\ \phi_{\ell,\mathfrak{l}}^{m_{i,\mathfrak{q}}/m_\ell} & \text{if } i \geqslant \ell = i(\mathfrak{q}, \mathfrak{l}). \end{cases}$$

By Lemma 5.19, the $\mathfrak{p}$-valuation of the resulting φ will not decrease, except possibly in the case where $\mathfrak{p} = \mathfrak{q}$. However, since $\varphi_{\mathfrak{q}} = \phi_{\mathfrak{q}}$, we may increase the $\mathfrak{q}$-valuation of $\varphi_{\mathfrak{q}}$ by choosing a better Okutsu approximation $\phi_{\mathfrak{q}}$ to compensate any decrease in value.

After this step we remove $\mathfrak{q}$ from S_0, since $\varphi_{\mathfrak{q}} = \phi_{\mathfrak{q}}$ and then return to Step 1.

As Step 3 reduces the number of prime ideals in S_0, this process will clearly end after at most $\#S$ iterations. □

6. Proof of Theorem 3.3

In the interest of clarity, we will only prove Theorem 3.3 in the case $I = \mathcal{O}_L$. The proof in the case of an arbitrary fractional ideal is almost identical. Further details on the required adaptations can be found in [13, Ch. 6].

6.1. **Precomputation.** Recall that our set S of prime ideals has a total ordering $S = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_s\}$ satisfying (8). Denote $n_S := \sum_{\mathfrak{p}\in S} n_{\mathfrak{p}}$, $w_S := w_{S,\mathcal{O}_L}$ and consider the following intervals of S:

$$[a,b] := \{\mathfrak{q}_j : a \leqslant j \leqslant b\}, \qquad 1 \leqslant a \leqslant b \leqslant s.$$

Definition 6.1. *An* order preserving *partition of S is a decomposition $S = I_1 \cup \cdots \cup I_t$ of S into the disjoint union of intervals $I_j = [a_j, b_j]$ with increasing end points $b_1 < \cdots < b_t$.*

Take extended families of numerators $g_{0,I_j}, \ldots, g_{n_j,I_j}$ of Okutsu I_j-bases, for all $1 \leqslant j \leqslant t$, where $n_j := n_{I_j}$. That is, each g_{i,I_j} has degree i, belongs to $\mathrm{Ok}(I_j)$ and $w_{I_j}\left(g_{i,I_j}\right)$ is maximal amongst all monic polynomials in $\mathcal{O}_v[x]$ of degree i.

Consider multi-indices $\mathbb{i} = (i_1, \ldots, i_t)$ of degree $\deg \mathbb{i} = i_1 + \cdots + i_t$ and monic polynomials $g_{\mathbb{i}} := g_{i_1,I_1} \cdots g_{i_t,I_t} \in \mathcal{O}[x]$.

We may consider the version of MaxMin presented in Algorithm 2.

Algorithm 2 MaxMin$[S = I_1 \cup \cdots \cup I_t]$ algorithm

Input: An order preserving partition $S = I_1 \cup \cdots \cup I_t$ of $S \subseteq \mathcal{P}$, and extended families $\left\{g_{i,I_j} : 0 \leqslant i \leqslant n_{I_j}\right\}$ of numerators of Okutsu I_j-bases for all $1 \leqslant j \leqslant t$.

Output: A family $\mathbb{i}_0, \mathbb{i}_1, \ldots, \mathbb{i}_{n_S} \in \mathbb{N}^t$ of multi-indices of degree $0, 1, \ldots, n_S$, respectively.

1: $\mathbb{i}_0 \leftarrow (0, \ldots, 0) \in \mathbb{N}^t$
2: **for** $k = 0 \to n_S - 1$ **do**
3: $\quad j \leftarrow \mathrm{Min}\left\{1 \leqslant i \leqslant t : w_{I_i}\left(g_{\mathbb{i}_k}\right) = w_S\left(g_{\mathbb{i}_k}\right)\right\}$
4: $\quad \mathbb{i}_{k+1} \leftarrow \mathbb{i}_k + \mathbb{u}_j$
5: **end for**

Such a decomposition of MaxMin will be useful for the proof of Theorem 3.3.

Definition 6.2. *For indices $1 \leqslant a \leqslant b \leqslant s$, we say that $I = [a,b]$* admits precomputation *if, after natural identifications, the algorithm* MaxMin$[S]$ *has the same output as*

$$\mathrm{MaxMin}\left[S = \{\mathfrak{q}_1\} \cup \cdots \cup \{\mathfrak{q}_{a-1}\} \cup I \cup \{\mathfrak{q}_{b+1}\} \cup \cdots \cup \{\mathfrak{q}_s\}\right], \tag{19}$$

where we consider the output of MaxMin$[I]$ *as an extended Okutsu I-basis.*

By "natural identifications" we mean that if the k-th output of MaxMin$[S]$ *is $\mathbb{i}_k = (i_{\mathfrak{q}_1}, \ldots, i_{\mathfrak{q}_s})$, then the k-th output of the algoritm* (19) *is:*

$$\mathbb{j}_k = (i_{\mathfrak{q}_1}, \ldots, i_{\mathfrak{q}_a-1}, i_I, i_{\mathfrak{q}_b+1}, \ldots, i_{\mathfrak{q}_s}),$$

while the i_I-th output of MaxMin$[I]$ *is $(i_{\mathfrak{q}_a}, \ldots, i_{\mathfrak{q}_b})$.*

The next result is an immediate consequence of the definition.

Lemma 6.3. *Let $S = I_1 \cup \cdots \cup I_t$ be an order preserving partition of S. If all intervals I_j admit precomputation, then* MaxMin$[S = I_1 \cup \cdots \cup I_t]$ *has the same output as* MaxMin$[S]$*, after natural identifications.* □

Let us give a criterion for an interval to admit precomputation.

Lemma 6.4. *Let* $\mathbb{i}_0, \mathbb{i}_1, \ldots, \mathbb{i}_{n_S}$ *be the output of* MaxMin$[S]$ *and let* $I \subseteq S$ *be an interval of* S*. For each* $0 \leqslant k \leqslant n_S$*, let* $\mathbb{i}_k = (i_{\mathfrak{q}})_{\mathfrak{q}\in S}$ *and denote*

$$g_{\mathbb{i}_k} = \prod_{\mathfrak{q}\in S} g_{i_{\mathfrak{q}},\mathfrak{q}}, \qquad G_{\mathbb{i}_k} = \prod_{\mathfrak{q}\in S\setminus I} g_{i_{\mathfrak{q}},\mathfrak{q}}.$$

Suppose that for each $0 \leqslant k \leqslant n_S$ *the following condition holds*

$$w_I\left(g_{\mathbb{i}_k}\right) = w_S\left(g_{\mathbb{i}_k}\right) \implies w_{\mathfrak{p}}\left(G_{\mathbb{i}_k}\right) = w_{\mathfrak{q}}\left(G_{\mathbb{i}_k}\right), \qquad \forall\ \mathfrak{p},\mathfrak{q}\in I.$$

Then, I *admits precomputation.*

Proof. Let $(\mathbb{i}_k)_{0\leqslant k\leqslant n_S}$ be the output of MaxMin$[S]$ and $(\mathbb{j}_k)_{0\leqslant k\leqslant n_S}$ be the output of the precomputed MaxMin algorithm (19).

Clearly, $\mathbb{i}_0$ and $\mathbb{j}_0$ may be identified. For $k \geqslant 0$, suppose that $\mathbb{i}_k$ may be identified with $\mathbb{j}_k$. This means

$$\begin{aligned}\mathbb{i}_k &= \left(i_{\mathfrak{q}_1}, \ldots, i_{\mathfrak{q}_s}\right),\\ \mathbb{j}_k &= \left(i_{\mathfrak{q}_1}, \ldots, i_{\mathfrak{q}_a-1}, i_I, i_{\mathfrak{q}_b+1}, \ldots, i_{\mathfrak{q}_s}\right),\end{aligned}$$

while the i_I-th output of MaxMin$[I]$ is the multi-index $\left(i_{\mathfrak{q}_j}\right)_{a\leqslant j\leqslant b}$.

Let $g'_0, \ldots, g'_{n_I}$ be the numerators deduced from the application of MaxMin$[I]$ and $g'_{\mathbb{j}_0}, \ldots, g'_{\mathbb{j}_{n_S}}$ the numerators deduced from (19). Clearly,

$$g'_{\mathbb{j}_k} = g'_{i_I} \prod_{\mathfrak{q}\in S\setminus I} g_{i_{\mathfrak{q}},\mathfrak{q}} = \prod_{\mathfrak{q}\in I} g_{i_{\mathfrak{q}},\mathfrak{q}} \prod_{\mathfrak{q}\in S\setminus I} g_{i_{\mathfrak{q}},\mathfrak{q}} = g_{\mathbb{i}_k}, \qquad g'_{i_I} = \prod_{m=a}^{b} g_{i_{\mathfrak{q}_m},\mathfrak{q}_m}.$$

The algorithm MaxMin$[S]$ outputs $\mathbb{i}_{k+1} = \mathbb{i}_k + \mathbb{u}_j$, where

$$j = \operatorname{Min}\left\{1 \leqslant m \leqslant s : w_{\mathfrak{q}_m}\left(g_{\mathbb{i}_k}\right) = w_S\left(g_{\mathbb{i}_k}\right)\right\}.$$

If $\mathfrak{q}_j \notin I$, then the $\mathfrak{q}_j$-index in $\mathbb{j}_k$ will also be the least index satisfying $w_{\mathfrak{q}_j}\left(g'_{\mathbb{j}_k}\right) = w_S\left(g'_{\mathbb{j}_k}\right)$, since $g'_{\mathbb{j}_k} = g_{\mathbb{i}_k}$. Thus, the algorithm in (19) will also increase the $\mathfrak{q}_j$-coordinate.

If $\mathfrak{q}_j \in I$, then $w_I\left(g_{\mathbb{i}_k}\right) = w_S\left(g_{\mathbb{i}_k}\right)$ and $w_{\mathfrak{q}_m}\left(g_{\mathbb{i}_k}\right) > w_S\left(g_{\mathbb{i}_k}\right)$ for all $m < a$; thus, (19) will increase i_I by one. In this case, we must show that the (i_I+1)-th output of MaxMin$[I]$ is the multi-index obtained from $\left(i_{\mathfrak{q}_j}\right)_{a\leqslant j\leqslant b}$ by increasing the $\mathfrak{q}_j$-coordinate by one.

The index increased by MaxMin$[I]$ will be:

$$J = \operatorname{Min}\left\{a \leqslant m \leqslant b : w_{\mathfrak{q}_m}\left(g'_{i_I}\right) = w_I\left(g'_{i_I}\right)\right\}.$$

By hypothesis, $\nu := w_{\mathfrak{q}}\left(G_{\mathbb{i}_k}\right)$ is independent of the choice of $\mathfrak{q} \in I$. Since $g_{\mathbb{i}_k} = G_{\mathbb{i}_k} g'_{i_I}$, we have:

$$w_{\mathfrak{q}}\left(g_{\mathbb{i}_k}\right) = w_{\mathfrak{q}}\left(g'_{i_I}\right) + \nu, \qquad \forall\ \mathfrak{q}\in I.$$

In particular, $w_S\left(g_{\mathbb{i}_k}\right) = w_I\left(g_{\mathbb{i}_k}\right) = w_I\left(g'_{i_I}\right) + \nu$, so that $J = j$. □

One specific case of precomputation which we will make use of, is the precomputation of certain intervals $S_{\mathbb{t}} \subseteq S$ defined by a type $\mathbb{t}$.

Lemma 6.5. *For any* $\mathbb{t} \in \mathfrak{T}$*, if the interval* $S_{\mathbb{t}}$ *is non-empty, it admits precomputation.*

Proof. For every $\mathfrak{p} \in S_{\mathfrak{t}}$ and every $\mathfrak{q} \notin S_{\mathfrak{t}}$, the explicit formulas from Proposition 2.3 show that $w_{\mathfrak{p}}(\phi_{i,\mathfrak{q}})$ is independent of $\mathfrak{p}$, for all i. Hence, the same is true for all polynomials $G_{\mathbb{i}_k}$ that are a product of these ϕ-polynomials.

Thus, $S_{\mathfrak{t}}$ meets the criterion of Lemma 6.4. □

In [13] we give concrete examples of intervals $I \subset S$ which do not admitprecomputation.

6.2. **The block-wise MaxMin algorithm.** Consider an ordered subset $S = \{\mathfrak{q}_1, \dots, \mathfrak{q}_s\} \subseteq \mathcal{P}$. Let $\mathfrak{T}_S$ be the tree gathering all the paths of all leaves $\mathfrak{t}_{\mathfrak{p}} \in \mathfrak{T}$ for $\mathfrak{p} \in S$. Take

$$\ell = i(S) := \operatorname{Min}\{i(\mathfrak{p}, \mathfrak{q}) : \mathfrak{p}, \mathfrak{q} \in S\}.$$

The tree $\mathfrak{T}_S$ is disconnected if and only if $\ell = 0$. Assume from now on that $\ell \geqslant 1$; in this case, $\ell - 1$ is the order of the greatest common node of all paths joining the leaves of $\mathfrak{T}_S$ with the root node. In this case, the Okutsu frames of all primes $\mathfrak{p} \in S$ have the same first $\ell - 1$ key polynomials $\phi_1, \dots, \phi_{\ell-1}$. Thus, the first m_ℓ numerators of the Okutsu $\mathfrak{p}$-bases coincide for all $\mathfrak{p} \in S$. Let

$$\mathcal{N} = \{1 = h_0, h_1, \dots, h_{m_\ell - 1}\},$$

be the family of these common numerators. Note that

$$w_{\mathfrak{p}}(h) = w_{\mathfrak{q}}(h), \qquad \forall\ \mathfrak{p}, \mathfrak{q} \in S,\ \forall\ h \in \mathcal{N}. \tag{20}$$

Lemma 6.6. *For all $\mathfrak{p}, \mathfrak{q} \in S$ and all $0 \leqslant r, t < m_\ell$:*

$$w_{\mathfrak{q}}(h_r h_t) \leqslant \begin{cases} w_{\mathfrak{q}}(h_{r+t}), & \text{if } r + t < m_\ell, \\ w_{\mathfrak{q}}(\phi_{\ell,\mathfrak{p}} h_k), & \text{if } r + t = m_\ell + k,\ k \geqslant 0. \end{cases}$$

Proof. By Lemma 5.17 (1), in any product of powers of $\phi_1, \dots, \phi_{\ell-1}$ we may replace $\phi_{i-1}^{e_{i-1} f_{i-1}}$ with $\phi_{i,\mathfrak{p}}$ to increase the $\mathfrak{q}$-valuation. This proves both inequalities. □

Lemma 6.7. *Let $\mathbb{i}$ be a maximal multi-index of degree divisible by m_ℓ.*

1. *There exists a maximal multi-index $\mathbb{i}' = (i'_{\mathfrak{p}})_{\mathfrak{p} \in S}$ of the same degree, having all its coordinates $i'_{\mathfrak{p}}$ divisible by m_ℓ.*
2. *All elements in the family $g_{\mathbb{i}}\mathcal{N}$ are maximal numerators.*

Proof. For $0 \leqslant j < m_\ell$, let $\mathbb{j} = (j_{\mathfrak{p}})_{\mathfrak{p} \in S}$ be a multi-index of degree $i m_\ell + j$. Each index $j_{\mathfrak{p}}$ may be written

$$j_{\mathfrak{p}} = q_{\mathfrak{p}} m_\ell + k_{\mathfrak{p}}, \qquad 0 \leqslant k_{\mathfrak{p}} < m_\ell,$$

and the numerators $g_{j_{\mathfrak{p}},\mathfrak{p}}$ of the Okutsu $\mathfrak{p}$-basis may be written

$$g_{j_{\mathfrak{p}},\mathfrak{p}} = G_{\mathfrak{p}} h_{k_{\mathfrak{p}}}, \qquad \deg G_{\mathfrak{p}} = q_{\mathfrak{p}} m_\ell.$$

Since all polynomials $G_{\mathfrak{p}}$ have a degree which is a multiple of m_ℓ, we have $\sum_{\mathfrak{p} \in S} k_{\mathfrak{p}} = q m_\ell + j$, for some non-negative integer q.

Let $g = \prod_{\mathfrak{p} \in S} G_{\mathfrak{p}}$ and choose any fixed prime ideal $\mathfrak{p}_0 \in S$. By (20), an iterative application of the inequalities in Lemma 6.6 shows that for any $\mathfrak{q} \in S$ we have

$$w_{\mathfrak{q}}(g_{\mathbb{j}}) = w_{\mathfrak{q}}\left(\prod_{\mathfrak{p} \in S} G_{\mathfrak{p}} h_{k_{\mathfrak{p}}}\right) = w_{\mathfrak{q}}(g) + w_{\mathfrak{q}}\left(\prod_{\mathfrak{p} \in S} h_{k_{\mathfrak{p}}}\right) \leqslant w_{\mathfrak{q}}(g) + w_{\mathfrak{q}}\left(\phi^q_{\ell,\mathfrak{p}_0} h_j\right).$$

Since this holds for all $\mathfrak{q} \in S$, we deduce that $w_S(g_{\mathbb{j}}) \leqslant w_S\left(g \phi^q_{\ell,\mathfrak{q}} h_j\right)$.

These arguments, applied to $\mathbb{j} = \mathbb{i}$ (and $j = 0$) prove item (1). Also, applied to an arbitrary $\mathbb{j}$ of degree $\deg(\mathbb{i}) + j$ show that

$$w_S(g_{\mathbb{j}}) \leqslant w_S\left(\phi^q_{\ell,\mathfrak{p}_0} \cdot g\right) + w_{\mathfrak{p}_0}(h_j) \leqslant w_S(g_{\mathbb{i}}) + w_{\mathfrak{p}_0}(h_j) = w_S(g_{\mathbb{i}} h_j),$$

by the maximality of $g_{\mathbb{i}}$. This proves item (2). □

Lemma 6.8. *Let $\mathbb{i} = (i_{\mathfrak{q}})_{\mathfrak{q}\in S}$ be an output multi-index of* MaxMin$[S]$ *of degree divisible by m_ℓ.*

(1) *All coordinates $i_{\mathfrak{q}}$ are divisible by m_ℓ.*
(2) *Let $j = \operatorname{Min}\{1 \leqslant m \leqslant s : w_{\mathfrak{q}_m}(g_{\mathbb{i}}) = w_S(g_{\mathbb{i}})\}$. Then, the next m_ℓ iterations of* MaxMin$[S]$ *increase the coordinate $\mathfrak{q}_j$.*

Proof. All coordinates of $\mathbb{i}_0$ are zero; hence divisible by m_ℓ. Thus, it suffices to prove that any output multi-index $\mathbb{i} = (i_{\mathfrak{q}})_{\mathfrak{q}\in S}$ whose coordinates are all divisible by m_ℓ satisfies (2).

Let $j = \operatorname{Min}\{1 \leqslant m \leqslant s : w_{\mathfrak{q}_m}(g_{\mathbb{i}}) = w_S(g_{\mathbb{i}})\}$. If $\mathbb{i} = \mathbb{i}_k$ is the k-th output multi-index of MaxMin$[S]$, the algorithm selects $\mathbb{i}_{k+1} = \mathbb{i}_k + \mathbb{u}_j$. Since $i_{\mathfrak{q}_j}$ is a multiple of m_ℓ, we have $g_{\mathbb{i}_{k+1}} = g_{\mathbb{i}_k} h_1$; hence,

$$w_{\mathfrak{q}}\left(g_{\mathbb{i}_{k+1}}\right) = w_{\mathfrak{q}}(g_{\mathbb{i}_k}) + w_{\mathfrak{q}}(h_1) \geqslant w_S(g_{\mathbb{i}_k}) + w_{\mathfrak{q}}(h_1) = w_S\left(g_{\mathbb{i}_{k+1}}\right),$$

for all $\mathfrak{q} \in S$. Thus, $w_{\mathfrak{q}}\left(g_{\mathbb{i}_{k+1}}\right) = w_S\left(g_{\mathbb{i}_{k+1}}\right)$ if and only if $w_{\mathfrak{q}}(g_{\mathbb{i}_k}) = w_S(g_{\mathbb{i}_k})$. Thus, the next iteration increases the $\mathfrak{q}_j$-coordinate again. By iterating this argument, we get $g_{\mathbb{i}_{k+m_\ell-1}} = g_{\mathbb{i}_k} h_{m_\ell-1}$. At this point, the $\mathfrak{q}_j$-coordinate will be increased once more to yield $\mathbb{i}_{k+m_\ell} = \mathbb{i}_k + m_\ell \mathbb{u}_j$. □

This result shows that MaxMin$[S]$ works by blocks of length m_ℓ. Thus, we may consider Algorithm 3, where we agree that $m_\ell = 1$ if $\mathfrak{T}_S$ is disconnected. Note that for $m_\ell = 1$, MaxMin$[S; m_\ell]$ coincides with MaxMin$[S]$.

Algorithm 3 MaxMin$[S; m_\ell]$ algorithm

Input: An ordered subset $S = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_s\} \subseteq \mathcal{P}$ and extended families $\{g_{i,\mathfrak{q}} : 0 \leqslant i \leqslant n_{\mathfrak{q}}\}$ of numerators of Okutsu $\mathfrak{q}$-bases of each $\mathfrak{q} \in S$.
Output: A family $\mathbb{i}_0, \mathbb{i}_{m_\ell}, \mathbb{i}_{2m_\ell}, \ldots, \mathbb{i}_{n_S/m_\ell}$ of multi-indices with $\deg \mathbb{i}_k = k$, having all coordinates divisible by m_ℓ.

```
i_0 ← (0, ..., 0)
for k = 0 → (n_S/m_ℓ) − 1 do
    j ← Min{ 1 ⩽ i ⩽ s : w_{q_i}(g_{i_{km_ℓ}}) = w_S(g_{i_{km_ℓ}}) }
    i_{(k+1)m_ℓ} ← i_{km_ℓ} + m_ℓ u_j
end for
```

Theorem 6.9. *The output multi-indices of* MaxMin$[S; m_\ell]$ *are maximal amongst all multi-indices of the same degree with coordinates divisible by m_ℓ.*

Theorem 3.3 follows from Theorem 6.9. In fact, by Lemma 6.7, all output multi-indices of MaxMin$[S; m_\ell]$ will be maximal and by Lemma 6.8 these multi-indices coincide with the output multi-indices of degree divisible by m_ℓ of MaxMin$[S]$.

Finally, Lemma 6.8 shows how to derive all intermediary output multi-indices of MaxMin$[S]$ and Lemma 6.7 shows that these multi-indices are maximal too.

6.3. **Branching cases.** The basic idea for the proof of Theorem 6.9 is to split $S = U \cup D$ (U for "up" and D for "down") into the disjoint union of two intervals which admit precomputation and then analyse the behaviour of MaxMin$[S = U \cup D]$ for which the multi-indices have only two coordinates.

Lemma 6.8 shows that the output multi-indices of MaxMin$[S; m_\ell]$ coincide with the output of an ordinary application of the 2-dimensional MaxMin applied to the precomputations MaxMin$[U; m_\ell]$ and MaxMin$[D; m_\ell]$. We shall denote this algorithm by MaxMin$[S = U \cup D; m_\ell]$.

We distinguish four cases according to the structure of the tree $\mathfrak{T}_S$:

Case (A). *The tree $\mathfrak{T}_S$ is disconnected, composed of t connected trees with root nodes $\psi_{0,1}, \dots, \psi_{0,t}$. We take D to be the connected component of $\mathfrak{T}_S$ with root node $\psi_{0,t}$.*

For $\mathfrak{T}_S$ connected, the proof of Theorem 6.9 makes use of the structure of the non-optimised tree with base type $\mathfrak{t}_{\ell-1}$ which is the greatest common node in all paths joining the leaves of $\mathfrak{T}_S$ with the root node.

Let ϕ_ℓ be the first representative of $\mathfrak{t}_{\ell-1}$ which leads to branching. Thus, before constructing ϕ_ℓ, the Montes algorithm may have constructed other representatives of $\mathfrak{t}_{\ell-1}$ admitting unibranch refinements.

Let $\lambda_{\min}$ be the least slope (in absolute size) occurring in the branching based on ϕ_ℓ. Let $S_{\min} \subseteq S$ be the subset of all prime ideals derived from branches of slope $\lambda_{\min}$ of ϕ_ℓ.

Case (B). *There exists a branch $\mathfrak{t}$ with slope $\lambda_{\min}$ which suffered refinement. In this case, we take $D = S_{\mathfrak{t}}$ to be the set of all prime ideals derived from this branch. Note that $\phi_{\ell,\mathfrak{p}} \neq \phi_\ell \ \forall\ \mathfrak{p} \in D$, and that there may be other $\lambda_{\min}$-branches.*

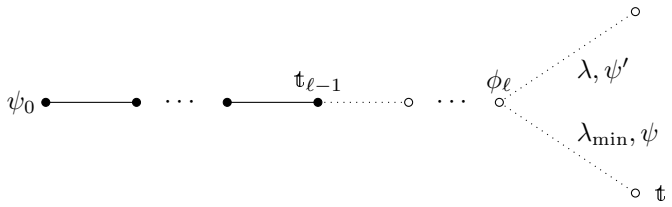


FIGURE 10. Case (B). Tree $\mathfrak{T}_S^{\text{nop}}$ with at least one refined $\lambda_{\min}$-branch.

Case (C). *None of the $\lambda_{\min}$-branches suffered refinement, and there are no other slopes. In other words, $\lambda_{\ell,\mathfrak{p}} = \lambda_{\min}$ and $\phi_{\ell,\mathfrak{p}} = \phi_\ell$ for all $\mathfrak{p} \in S$.*

In this case, we take $D = S_{\mathfrak{t}}$, for any choice of a $\lambda_{\min}$-branch $\mathfrak{t}$.

Case (D). *None of the $\lambda_{\min}$-branches suffered refinement, but there are other slopes. In other words, $\lambda_{\ell,\mathfrak{p}} = \lambda_{\min}$ and $\phi_{\ell,\mathfrak{p}} = \phi_\ell$, for all $\mathfrak{p} \in S_{\min} \subsetneq S$.*

In this case, we take $D = S_{\min}$.

In all cases, we may change the ordering of $\mathcal{P}$ so that D and $U = S \backslash D$ are intervals.

6.3.1. *Proof of Theorem 6.9 in cases (A), (B) and (C).* Denote

$$c := \begin{cases} \dfrac{V_\ell + \lambda_{\min}}{e_1 \cdots e_{\ell-1}}, & \text{if } \mathfrak{T}_S \text{ is connected,} \\ 0, & \text{if } \mathfrak{T}_S \text{ is disconnected.} \end{cases}$$

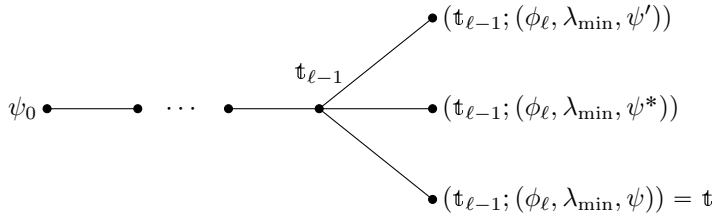


FIGURE 11. Case (C). Tree $\mathfrak{T}_S$ with only unrefined $\lambda_{\min}$-branches.

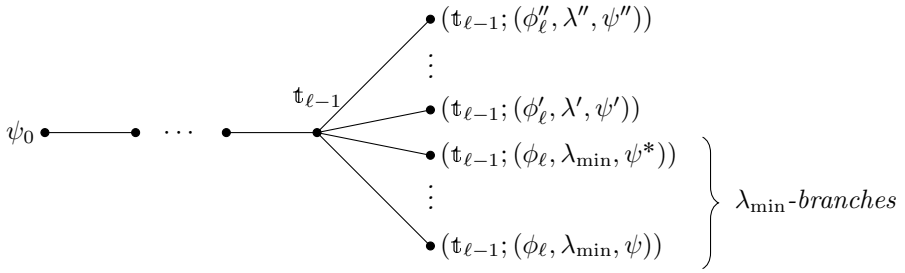


FIGURE 12. Case (D). Tree $\mathfrak{T}_S$ with with unrefined $\lambda_{\min}$-branches and other slopes.

The explicit formulas from Proposition 2.3 show that

$$w_{\mathfrak{p}}(\phi_{m,\mathfrak{q}}) = (m/m_\ell)c = w_{\mathfrak{q}}(\phi_{m,\mathfrak{p}}), \qquad \forall\ \mathfrak{p} \in U,\ \mathfrak{q} \in D,\ \forall\ m \geqslant \ell. \tag{21}$$

On the other hand, all ideas and criteria about precomputation apply to the MaxMin algorithms restricted to all multi-indices whose coordinates are divisible by m_ℓ. Hence, (21) shows that D and $U = S \backslash D$ meet the condition of Lemma 6.4 and both intervals admit precomputation.

Denote the respective output families of numerators of MaxMin$[U; m_\ell]$ and MaxMin$[D; m_\ell]$ by:

$$1, g_1, \ldots, g_{n_U/m_\ell}; \qquad 1, g'_1, \ldots, g'_{n_D/m_\ell}.$$

Note that $\deg g_k = km_\ell$, for all $k \leqslant n_U/m_\ell$ and $\deg g'_k = km_\ell$, for all $k \leqslant n_D/m_\ell$.

By Lemma 6.3, MaxMin$[S; m_\ell]$ has the same output as MaxMin$[S = U \cup D; m_\ell]$, after natural identifications of the respective multi-indices. In other words, if (i, j) is the k-th output of MaxMin$[S = U \cup D; m_\ell]$ (so that $k = i + j$), then the k-th numerator provided by MaxMin$[S; m_\ell]$ is $g_i g'_j$.

Definition 6.10. *We say that a monic polynomial $G \in \mathcal{O}[x]$* has support *in a subset $S' \subset S$ if it is a product of polynomials $\phi_{m,\mathfrak{p}}$ for $\mathfrak{p} \in S'$ and $m \geqslant \ell$.*

Note that the degree of G is necessarily a multiple of m_ℓ.

In order to prove Theorem 6.9, we must show that the output numerators of MaxMin$[S; m_\ell]$ are maximal amongst all polynomials of the same degree with support in S.

We proceed by induction on $\#S$. The case $\#S = 1$ being trivial, we may assume by the induction hypothesis that both sequences of numerators are maximal amongst all polynomials of the same degree with support in U and D, respectively.

For all $0 \leqslant i \leqslant n_U/m_\ell$ and all $0 \leqslant j \leqslant n_D/m_\ell$, denote

$$\nu_i := w_U(g_i) - ic, \qquad \nu'_j := w_D(g'_j) - jc. \tag{22}$$

We agree that $\nu_{-1} = \nu'_{-1} = -1$.

Lemma 6.11. *For all $i, j \geqslant 0$,*

$$\nu_i \leqslant \nu_{i+1}, \qquad \nu'_j \leqslant \nu'_{j+1}.$$

Proof. By Proposition 2.3, $w_{\mathfrak{q}}(\phi_{\ell,\mathfrak{q}}(\theta)) = (V_\ell + \lambda_{\ell,\mathfrak{q}})/(e_1 \cdots e_{\ell-1})$ for all $\mathfrak{q} \in U$. Since $\lambda_{\ell,\mathfrak{q}} \geqslant \lambda_{\min}$, the maximality of g_{i+1} implies

$$w_U(g_{i+1}) \geqslant w_U(g_i\phi_{\ell,\mathfrak{q}}) \geqslant w_U(g_i) + c, \qquad \forall\ \mathfrak{q} \in U.$$

Similarly, the maximality of g'_{j+1} implies

$$w_D(g'_{j+1}) \geqslant w_D(g'_j\phi_\ell) = w_D(g'_j) + c.$$

By the definition (22) of ν_i, ν'_j, this ends the proof of the lemma. □

For any bi-index $\mathfrak{i} = (i, j)$, and any $\mathfrak{p} \in U$, $\mathfrak{q} \in D$, (21) shows that

$$\begin{aligned} w_U(g_{\mathfrak{i}}) &= w_U(g_i) + jc = \nu_i + (i+j)c = \nu_i + (\deg \mathfrak{i})c, \\ w_D(g_{\mathfrak{i}}) &= w_D(g'_j) + ic = \nu'_j + (i+j)c = \nu'_j + (\deg \mathfrak{i})c, \\ w_S(g_{\mathfrak{i}}) &= w_S(g_ig'_j) = \operatorname{Min}\{\nu_i, \nu'_j\} + (\deg \mathfrak{i})c. \end{aligned}$$

Therefore, these numbers ν_i, ν'_j determine the flow of $\operatorname{MaxMin}[S = U \cup D; m_\ell]$. If (i, j) is an output pair, the next output pair is decided as follows:

$$\begin{aligned} w_U(g_ig'_j) = w_S(g_ig'_j) &\iff \nu_i \leqslant \nu'_j, && \text{“}U\text{-minimal”}, \\ w_D(g_ig'_j) = w_S(g_ig'_j) &\iff \nu'_j < \nu_i, && \text{“}D\text{-minimal”}. \end{aligned}$$

The next output pair is $(i+1, j)$ in the U-minimal case, and $(i, j+1)$ in the D-minimal case.

Proposition 6.12. *The output bi-indices (i, j) of $\operatorname{MaxMin}[S = U \cup D; m_\ell]$ satisfy the following properties:*

1. *Either $\nu'_{j-1} \leqslant \nu_i \leqslant \nu'_j$, or $\nu_{i-1} \leqslant \nu'_j < \nu_i$.*
2. *The output multi-indices of $\operatorname{MaxMin}[S = U \cup D; m_\ell]$ are maximal amongst all polynomials of the same degree with suppose in S.*

Proof. Clearly, the initial output pair $(0, 0)$ satisfies (1). Let us check that if an output pair (i, j) satisfies (1), then the next output pair satisfies (1) as well.

Suppose that $\nu'_{j-1} \leqslant \nu_i \leqslant \nu'_j$, so that the next output pair is $(i+1, j)$.

$$\begin{aligned} \nu_{i+1} \leqslant \nu'_j &\implies \nu'_{j-1} \leqslant \nu_i \leqslant \nu_{i+1} \leqslant \nu'_j, \\ \nu_{i+1} > \nu'_j &\implies \nu_i \leqslant \nu'_j < \nu_{i+1}. \end{aligned}$$

Suppose that $\nu_{i-1} \leqslant \nu'_j < \nu_i$, so that the next output pair is $(i, j+1)$.

$$\begin{aligned} \nu_i \leqslant \nu'_{j+1} &\implies \nu'_j < \nu_i \leqslant \nu'_{j+1}, \\ \nu_i > \nu'_{j+1} &\implies \nu_{i-1} \leqslant \nu'_j \leqslant \nu'_{j+1} < \nu_i. \end{aligned}$$

This proves item (1). As a consequence, for any $k \in \mathbb{Z}$ such that $0 \leqslant i - k \leqslant n_U/m_\ell$ and $0 \leqslant j + k \leqslant n_D/m_\ell$, we have:

$$\operatorname{Min}\{\nu_{i-k}, \nu'_{j+k}\} \leqslant \operatorname{Min}\{\nu_i, \nu'_j\}. \tag{23}$$

In fact, if $\nu'_{j-1} \leqslant \nu_i \leqslant \nu'_j$, then $\operatorname{Min}\left\{\nu_{i-k}, \nu'_{j+k}\right\} \leqslant \nu_i$, whereas in the case $\nu_{i-1} \leqslant \nu'_j < \nu_i$, we have $\operatorname{Min}\left\{\nu_{i-k}, \nu'_{j+k}\right\} \leqslant \nu'_j$.

In order to prove (2), suppose that (i, j) is an output pair of $\operatorname{MaxMin}[S = U \cup D; m_\ell]$ and let g be a polynomial of degree $(i+j)m_\ell$ with support in S. We may write $g = GG'$, with G, G' polynomials with support in U and D, respectively.

Suppose $\deg G = (i-k)m_\ell$, $\deg G' = (j+k)m_\ell$, for certain $k \in \mathbb{Z}$. By (21) and the maximality of the numerators g_{i-k}, g'_{j+k}, we have:

$$\begin{aligned} w_U(g) &= w_U\left(GG'\right) = w_U(G) + (j+k)c \\ &\leqslant \nu_{i-k} + (i-k)c + (j+k)c = \nu_{i-k} + (i+j)c, \end{aligned}$$

$$\begin{aligned} w_D(g) &= w_D\left(GG'\right) = w_D\left(G'\right) + (i-k)c \\ &\leqslant \nu'_{j+k} + (j+k)c + (i-k)c = \nu'_{j+k} + (i+j)c. \end{aligned}$$

Hence, by using (23), we get:

$$\begin{aligned} w_S(g) &= \operatorname{Min}\left\{w_U(g), w_D(g)\right\} = \operatorname{Min}\left\{\nu_{i-k}, \nu'_{j+k}\right\} + (i+j)c \\ &\leqslant \operatorname{Min}\left\{\nu_i, \nu'_j\right\} + (i+j)c = w_S\left(g_i g'_j\right). \end{aligned}$$ □

This ends the proof of Theorem 6.9 in cases (A), (B) and (C).

6.3.2. *Precomputation in Case (D).* Recall that $D = S_{\min}$ and $U = S \backslash D$. In this case, we have:

$$\phi_{\ell,\mathfrak{q}} = \phi_\ell = \phi(\mathfrak{p}, \mathfrak{q}), \qquad \forall\ \mathfrak{p} \in U, \mathfrak{q} \in D.$$

For each $\mathfrak{p} \in S$ we denote by $\lambda_\mathfrak{p}$ the slope of the branch of ϕ_ℓ in the non-optimised tree to which the leaf of $\mathfrak{p}$ belongs. Also, we denote

$$c := \frac{V_\ell + \lambda_{\min}}{e_1 \cdots e_{\ell-1}}, \qquad \delta_\mathfrak{p} := \frac{\lambda_\mathfrak{p} - \lambda_{\min}}{e_1 \cdots e_{\ell-1}} \geqslant 0.$$

The explicit formulas presented in Proposition 2.3 show that for all $\mathfrak{p} \in U, \mathfrak{q} \in D$:

$$\begin{aligned} &w_\mathfrak{q}(\phi_{i,\mathfrak{p}}) = (m_i/m_\ell)c, && \forall\ i \geqslant \ell, \\ &w_\mathfrak{p}(\phi_{i,\mathfrak{q}}) = \begin{cases} (m_i/m_\ell)c, & \text{if } i > \ell, \\ \delta_\mathfrak{p} + c, & \text{if } i = \ell. \end{cases} \end{aligned} \tag{24}$$

Let G be a polynomial of degree im_ℓ with support in U, and let G' be a polynomial of degree jm_ℓ with support in D. If $m := \operatorname{ord}_{\phi_\ell}(G')$, the formulas (24) show that:

$$\begin{aligned} w_U\left(GG'\right) &= \operatorname{Min}\left\{w_\mathfrak{p}(G) + m\delta_\mathfrak{p}\right\}_{\mathfrak{p} \in U} + jc, \\ w_D\left(GG'\right) &= w_D\left(G'\right) + ic. \end{aligned} \tag{25}$$

The first formula of (24) shows that D meets the criterion of Lemma 6.4 and admits precomputation. In order to show that U admits precomputation too, we need another lemma.

Notation. *For each $\mathfrak{p} \in D$, we denote $m_\mathfrak{p} := m_{\ell+1,\mathfrak{p}} = e_{\ell,\mathfrak{p}} f_{\ell,\mathfrak{p}} m_\ell$.*

Lemma 6.13. *Let $\mathbb{i} = (i_\mathfrak{p})_{\mathfrak{p} \in S}$ be an output of $\operatorname{MaxMin}[S; m_\ell]$ and $g = g_\mathbb{i}$ the corresponding numerator. Let $\mathfrak{p} \in S$ be the least prime with $w_\mathfrak{p}(g) = w_S(g)$.*

(1) *If* $\mathfrak{p} \in D$ *and* $m_{\mathfrak{p}} \mid i_{\mathfrak{p}}$*, then the next* $e_{\ell,\mathfrak{p}} f_{\ell,\mathfrak{p}}$ *output numerators are*

$$g\phi_\ell,\ g\phi_\ell^2,\ \ldots,\ g\phi_\ell^{e_{\ell,\mathfrak{p}} f_{\ell,\mathfrak{p}}-1},$$

and finally

$$\left(\prod_{\mathfrak{q}\neq\mathfrak{p}} g_{i_{\mathfrak{q}},\mathfrak{q}}\right)\cdot g_{i_{\mathfrak{p}}+m_{\mathfrak{p}},\mathfrak{p}}.$$

(2) *If* $\mathfrak{p} \in U$*, then* $m_{\mathfrak{q}} \mid i_{\mathfrak{q}}$ *for all* $\mathfrak{q} \in D$*.*

Proof. Suppose $\mathfrak{p} \in D$ and $m_{\mathfrak{p}} \mid i_{\mathfrak{p}}$. Since the element $g_{i_{\mathfrak{p}},\mathfrak{p}}$, a numerator of the Okutsu $\mathfrak{p}$-basis, has degree divisible by $m_{\mathfrak{p}}$, it is not divisible by ϕ_ℓ, and $g_{i_{\mathfrak{p}}+1,\mathfrak{p}} = g_{i_{\mathfrak{p}},\mathfrak{p}}\phi_\ell$. Hence, the next output numerator is $g\phi_\ell$.

By (24), $w_{\mathfrak{p}}(g\phi_\ell) = w_{\mathfrak{p}}(g) + c$, while $w_{\mathfrak{q}}(g\phi_\ell) \geqslant w_{\mathfrak{q}}(g) + c$ for all $\mathfrak{q} \in S$. Thus, the least prime with $w_{\mathfrak{q}}(g\phi_\ell) = w_S(g\phi_\ell)$ is, once again, the prime $\mathfrak{p}$.

This argument may be iterated as long as $\operatorname{ord}_{\phi_\ell}(g_{i_{\mathfrak{p}}+km_\ell,\mathfrak{p}}) = k < e_{\ell,\mathfrak{p}} f_{\ell,\mathfrak{p}}$. For $k = e_{\ell,\mathfrak{p}} f_{\ell,\mathfrak{p}} - 1$, the prime $\mathfrak{p}$ is still the least one satisfying $w_{\mathfrak{p}}\left(g\phi_\ell^k\right) = w_S\left(g\phi_\ell^k\right)$, so that the component of the multi-index corresponding to $\mathfrak{p}$ is increased and the output multi-index is $\mathbb{i} + m_{\mathfrak{p}}\mathbb{u}_{\mathfrak{p}}$.

The second item follows immediately from the first. □

Corollary 6.14. *U admits precomputation.*

Proof. Let us show that U meets the criterion of Lemma 6.4.

Let $\mathbb{i} = (i_{\mathfrak{p}})_{\mathfrak{p}\in S}$ be an output of MaxMin$[S; m_\ell]$ and let $g = g_{\mathbb{i}}$ be the corresponding numerator. Suppose that $w_U(g) = w_S(g)$. With respect to the ordering of S, all elements in U are less than all elements in D; hence, the least prime $\mathfrak{p}$ with $w_{\mathfrak{p}}(g) = w_S(g)$ belongs to U. By (2) of Lemma 6.13, $m_{\mathfrak{q}} \mid i_{\mathfrak{q}}$ for all $\mathfrak{q} \in D$, and this implies that none of the numerators $g_{i_{\mathfrak{q}},\mathfrak{q}}$, for $\mathfrak{q} \in D$, is divisible by ϕ_ℓ.

Therefore, (24) shows that $w_{\mathfrak{p}}\left(g_{i_{\mathfrak{q}},\mathfrak{q}}\right) = (i_{\mathfrak{q}}/m_\ell)c$ for all $\mathfrak{p} \in U$, and the value $w_{\mathfrak{p}}(G_{\mathbb{i}}) = w_{\mathfrak{p}}\left(\prod_{\mathfrak{q}\in D} g_{i_{\mathfrak{q}},\mathfrak{q}}\right)$ is independent of $\mathfrak{p} \in U$. □

6.3.3. *Proof of Theorem 6.9 in Case (D).* Denote the respective output families of numerators of MaxMin$[U; m_\ell]$ and MaxMin$[D; m_\ell]$ by:

$$1, g_1, \ldots, g_{n_U/m_\ell}; \qquad 1, g'_1, \ldots, g'_{n_D/m_\ell}.$$

Note that $\deg g_k = km_\ell$, for all $k \leqslant n_U/m_\ell$ and $\deg g'_k = km_\ell$ for all $k \leqslant n_D/m_\ell$.

Let $\mathbb{i} = (i_{\mathfrak{p}})_{\mathfrak{p}\in S}$ be an output of MaxMin$[S; m_\ell]$. Since U and D admit precomputation, Lemma 6.3 shows that $g_{\mathbb{i}} = g_i g'_j$, for the k-th output (i, j) of MaxMin$[S = U \cup D; m_\ell]$.

Notation. *We denote* $[j] := \operatorname{ord}_{\phi_\ell}(g'_j)$*, for* $0 \leqslant j \leqslant n_D/m_\ell$*.*

By Lemma 6.13, all indices $i_{\mathfrak{q}}$, for $\mathfrak{q} \in D$ are divisible by $m_{\mathfrak{q}}$ except eventually for one, say $i_{\mathfrak{q}_0}$. Hence, $[j]$ is the residue of the euclidian division of $i_{\mathfrak{q}_0}$ by $m_{\mathfrak{q}_0}$. Note that $[j] = 0$ if and only if $m_{\mathfrak{q}} \mid i_{\mathfrak{q}}$ for all $\mathfrak{q} \in D$.

Consider rational numbers ν_i, ν'_j as in (22). The formulas (25) translate into

$$\begin{aligned} w_U\left(g_i g'_j\right) &= \operatorname{Min}\left\{w_{\mathfrak{p}}(g_i) + [j]\delta_{\mathfrak{p}}\right\}_{\mathfrak{p}\in U} + jc, \\ w_D\left(g_i g'_j\right) &= w_D\left(g'_j\right) + ic = \nu'_j + (i+j)c. \end{aligned} \tag{26}$$

Lemma 6.15. *These data* ν_i, ν'_j *satisfy the following properties for all* $i, j > 0$*:*

(1) $\nu_{i-1} < \nu_i$.
(2) $\nu'_{j-1} \leqslant \nu'_j$ *and if* $[j] \neq 0$ *then equality holds.*

Proof. Take any $\mathfrak{p} \in U$. By Proposition 2.3, $w_{\mathfrak{p}}(\phi_{\ell,\mathfrak{p}}) = (V_\ell + \lambda_{\ell,\mathfrak{p}})/(e_1 \cdots e_{\ell-1}) > c$, since $\lambda_{\ell,\mathfrak{q}} > \lambda_{\min}$. The maximality of g_i implies

$$w_U(g_i) \geqslant w_U(g_{i-1}\phi_{\ell,\mathfrak{p}}) > w_U(g_{i-1}) + c.$$

This proves (1). Similarly, the maximality of g'_j implies $\nu'_{j-1} \leqslant \nu'_j$.

By Lemma 6.13, $[j] \neq 0$ implies that $g'_j = g'_{j-1}\phi_\ell$. Since $w_{\mathfrak{q}}(\phi_\ell) = c$ for all $\mathfrak{q} \in D$, this implies $w_D\left(g'_j\right) = w_D\left(g'_{j-1}\right) + c$. This proves (2). □

Lemma 6.16. *Let* $\mathbb{i} = (i, j)$ *be an output pair of* $\mathrm{MaxMin}[S = U \cup D; m_\ell]$. *Then,*

(1) *Either* $\nu'_{j-1} \leqslant \nu_i \leqslant \nu'_j$, *or* $\nu_{i-1} \leqslant \nu'_j < \nu_i$.
(2) *The next output pair is* $(i+1, j)$ *in the first case, and* $(i, j+1)$ *in the second case.*

Proof. Clearly, the initial pair $(0, 0)$ satisfies (1), the next output pair is $(1, 0)$, and it satisfies (1) too. Let us show by induction that if an output pair satisfies (1) then the next output pair is given as indicated in (2) and it satisfies (1) as well.

Suppose that $\nu'_{j-1} \leqslant \nu_i \leqslant \nu'_j$. If the previous output pair was $(i-1, j)$, the induction hypothesis implies that we had $\nu'_{j-1} \leqslant \nu_{i-1} \leqslant \nu'_j$. Since $\nu'_{j-1} \leqslant \nu_{i-1} < \nu_i \leqslant \nu'_j$, we have $[j] = 0$ by item (2) of Lemma 6.15. If the previous output pair was $(i, j-1)$, then $\nu'_{j-1} < \nu_i$ by the induction hypothesis. This leads again to $\nu'_{j-1} < \nu'_j$ and to $[j] = 0$. Thus, (26) shows that

$$\begin{aligned} w_U\left(g_i g'_j\right) &= w_U(g_i) + jc = \nu_i + (i+j)c \\ &\leqslant \nu'_j + (i+j)c = w_D\left(g_i g'_j\right). \end{aligned}$$

Thus, $w_U\left(g_i g'_j\right) = w_S\left(g_i g'_j\right)$ and the next output pair is $(i+1, j)$. The arguments of the proof of Proposition 6.12 show that $(i+1, j)$ satisfies (1).

Suppose that $\nu_{i-1} \leqslant \nu'_j < \nu_i$. By (26), we have

$$\begin{aligned} w_D\left(g_i g'_j\right) &= \nu'_j + (i+j)c < \nu_i + (i+j)c \\ &= w_U(g_i) + jc = w_U\left(g_i g'_j\right). \end{aligned}$$

Thus, $w_D\left(g_i g'_j\right) = w_S\left(g_i g'_j\right)$ and the next output pair is $(i, j+1)$. The arguments of the proof of Proposition 6.12 show that $(i, j+1)$ satisfies (1). □

Lemma 6.17. *Consider indices* $0 \leqslant k \leqslant i$ *and let* G *be a polynomial of degree* $(i-k)m_\ell$ *with support in* U. *Then,*

$$\mathrm{Min}\left\{w_{\mathfrak{p}}(G) + k\delta_{\mathfrak{p}}\right\}_{\mathfrak{p}\in U} \leqslant \nu_i + (i-k)c.$$

Proof. Let $\mathfrak{q} \in U$ be a prime ideal with a maximal value of $\lambda_{\mathfrak{q}}$. The statement follows from the following chain of inequalities:

$$\mathrm{Min}\left\{w_{\mathfrak{p}}(G) + k\delta_{\mathfrak{p}}\right\}_{\mathfrak{p}\in U} + kc \leqslant w_U\left(G\phi^k_{\ell,\mathfrak{q}}\right) \leqslant w_U(g_i) = \nu_i + ic. \tag{27}$$

The second inequality of (27) follows from the maximality of g_i. The first inequality is deduced from the formulas from Proposition 2.3. In fact, for any $\mathfrak{p} \in U$,

these formulas yield $w_{\mathfrak{p}}\left(\phi_{\ell,\mathfrak{q}}\right) = (V_\ell + \lambda)/(e_1 \cdots e_{\ell-1})$, for a certain rational number λ, depending on $\mathfrak{p}$, such that $\lambda \geqslant \lambda_{\mathfrak{p}}$; hence,

$$\begin{aligned} w_{\mathfrak{p}}\left(G\phi_{\ell,\mathfrak{q}}^k\right) &= w_{\mathfrak{p}}\left(G\right) + k\frac{V_\ell + \lambda}{e_1 \cdots e_{\ell-1}} \\ &\geqslant w_{\mathfrak{p}}\left(G\right) + k(c + \delta_{\mathfrak{p}}), \end{aligned}$$

for all $\mathfrak{p} \in U$, which implies the first inequality in (27).

More precisely, if $i(\mathfrak{p},\mathfrak{q}) = \ell$, then $\lambda = \lambda_{\mathfrak{p}}^{\mathfrak{q}}$ or $\lambda = \operatorname{Min}\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\}$, according to $\phi(\mathfrak{p},\mathfrak{q})$ being equal to $\phi_{\ell,\mathfrak{q}}$ or not. Now, if $\mathfrak{p}$ and $\mathfrak{q}$ belong to the same ϕ_ℓ-branch of the non-optimised tree, we have (see Definition 5.11)

$$\lambda_{\mathfrak{p}} = \lambda_{\mathfrak{q}} < \operatorname{Min}\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\} \leqslant \lambda.$$

If $\mathfrak{p}$ and $\mathfrak{q}$ belong to different ϕ_ℓ-branches of the non-optimised tree, then $\lambda_{\mathfrak{p}}^{\mathfrak{q}} = \lambda_{\mathfrak{p}}$, $\lambda_{\mathfrak{q}}^{\mathfrak{p}} = \lambda_{\mathfrak{q}}$, so that, again,

$$\lambda_{\mathfrak{p}} = \operatorname{Min}\left\{\lambda_{\mathfrak{p}}, \lambda_{\mathfrak{q}}\right\} = \operatorname{Min}\left\{\lambda_{\mathfrak{p}}^{\mathfrak{q}}, \lambda_{\mathfrak{q}}^{\mathfrak{p}}\right\} \leqslant \lambda.$$

Finally, if $i(\mathfrak{p},\mathfrak{q}) > \ell$, then $\lambda = \lambda_{\ell,\mathfrak{q}} = \lambda_{\ell,\mathfrak{p}} \geqslant \lambda_{\mathfrak{p}}$, by Remark 5.12. □

We are ready to prove Theorem 6.9 in Case (D).

Proposition 6.18. *In Case (D), all output multi-indices of* $\operatorname{MaxMin}[S; m_\ell]$ *are maximal amongst the multi-indices of the same degree whose coordinates are all divisible by* m_ℓ.

Proof. Let $\mathbb{i} = (i_{\mathfrak{p}})_{\mathfrak{p}\in S}$ be an output multi-index of $\operatorname{MaxMin}[S; m_\ell]$, obtained by joining the i-th output of $\operatorname{MaxMin}[U]$ and the j-th output of $\operatorname{MaxMin}[D]$.

Let g be a polynomial of degree $(i+j)m_\ell$ with support in S. We may write $g = GG'$, with G, G' polynomials with support in U and D, respectively.

Suppose $\deg G = (i-k)m_\ell$, $\deg G' = (j+k)m_\ell$, for certain $k \in \mathbb{Z}$. Let us write

$$G' = H\phi_\ell^m, \qquad\qquad \phi_\ell \nmid H,\ \deg H = qm_\ell.$$

Note that $q + m = j + k$. By (25),

$$\begin{aligned} w_U\left(GG'\right) &= \operatorname{Min}\left\{w_{\mathfrak{p}}\left(G\right) + m\delta_{\mathfrak{p}}\right\}_{\mathfrak{p}\in U} + (j+k)c, \\ w_D\left(GG'\right) &= w_D\left(G'\right) + (i-k)c. \end{aligned}$$

Since $w_{\mathfrak{p}}\left(\phi_\ell\right) = c$ for all $\mathfrak{q} \in D$, the last equality leads to

$$\begin{aligned} w_D\left(GG'\right) &= w_D\left(H\right) + (m+i-k)c \leqslant w_D\left(g_q'\right) + (m+i-k)c \\ &= \nu_q' + (q+m+i-k)c = \nu_q' + (i+j)c. \end{aligned} \tag{28}$$

By Lemma 6.16, we may distinguish two cases according to the comparison of ν_i with ν_j'.

Case 1. $\nu_{j-1}' \leqslant \nu_i \leqslant \nu_j'$. In this case, we saw during the proof of Lemma 6.16 that $[j] = 0$. Hence, $w_S\left(g_i g_j'\right) = w_U\left(g_i g_j'\right) = \nu_i + (i+j)c$, by (26). We want to show that

$$w_S\left(GG'\right) = \operatorname{Min}\left\{w_U\left(GG'\right), w_D\left(GG'\right)\right\} \leqslant \nu_i + (i+j)c.$$

If $m \leqslant k$, then Lemma 6.17 shows that

$$\begin{aligned} w_U\left(GG'\right) &= \operatorname{Min}\left\{w_{\mathfrak{p}}\left(G\right) + m\delta_{\mathfrak{p}}\right\}_{\mathfrak{p}\in U} + (j+k)c \\ &\leqslant \operatorname{Min}\left\{w_{\mathfrak{p}}\left(G\right) + k\delta_{\mathfrak{p}}\right\}_{\mathfrak{p}\in U} + (j+k)c \\ &\leqslant \nu_i + (i-k)c + (j+k)c = \nu_i + (i+j)c. \end{aligned}$$

If $m > k$, then $q < j$, or equivalently $q \leqslant j-1$. Thus, (28) shows that

$$w_D\left(GG'\right) \leqslant \nu'_q + (i+j)c \leqslant \nu'_{j-1} + (i+j)c \leqslant \nu_i + (i+j)c.$$

Case 2. $\nu_{i-1} \leqslant \nu'_j < \nu_i$. In this case, we saw during the proof of Lemma 6.16 that $w_S\left(g_i g'_j\right) = w_D\left(g_i g'_j\right) = \nu'_j + (i+j)c$. We want to show that

$$w_S\left(GG'\right) = \operatorname{Min}\left\{w_U\left(GG'\right), w_D\left(GG'\right)\right\} \leqslant \nu'_j + (i+j)c.$$

If $m < k$, then $m \leqslant k-1$. Having in mind that $\deg G/m_\ell = i-k = (i-1)-(k-1)$, Lemma 6.17 shows that

$$\begin{aligned} w_U\left(GG'\right) &= \operatorname{Min}\left\{w_{\mathfrak{p}}\left(G(\theta)\right) + m\delta_{\mathfrak{p}}\right\}_{\mathfrak{p}\in U} + (j+k)c \\ &\leqslant \operatorname{Min}\left\{w_{\mathfrak{p}}\left(G(\theta)\right) + (k-1)\delta_{\mathfrak{p}}\right\}_{\mathfrak{p}\in U} + (j+k)c \\ &\leqslant \nu_{i-1} + (i-k)c + (j+k)c = \nu_{i-1} + (i+j)c \leqslant \nu'_j + (i+j)c. \end{aligned}$$

If $m \geqslant k$, then $q \leqslant j$ and (28) shows that

$$w_D\left(GG'\right) \leqslant \nu'_q + (i+j)c \leqslant \nu'_j + (i+j)c.$$

□

References

[1] Jens-Dietrich Bauch. *Lattices over polynomial Rings and Applications to Function Fields*. PhD thesis, Universitat Autònoma de Barcelona, July 2014.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Julio Fernández, Jordi Guàrdia, Jesús Montes, and Enric Nart. Residual ideals of MacLane valuations. *Journal of Algebra*, 427:30–75, April 2015.

[4] Jordi Guàrdia, Jesús Montes, and Enric Nart. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *Journal de Théorie des Nombres de Bordeaux*, 23(3):667–696, 2011.

[5] Jordi Guàrdia, Jesús Montes, and Enric Nart. Newton polygons of higher order in algebraic number theory. *Transactions of the American Mathematical Society*, 364:361–416, 2012.

[6] Jordi Guàrdia, Jesús Montes, and Enric Nart. A new computational approach to ideal theory in number fields. *Foundations of Computational Mathematics*, 13(5):729–762, 2013.

[7] Jordi Guàrdia, Jesús Montes, and Enric Nart. Higher Newton polygons and integral bases. *Journal of Number Theory*, 147:549–589, February 2015.

[8] Jordi Guàrdia and Enric Nart. Genetics of polynomials over local fields. In Stéphane Ballet, Marc Perret, and Alexey Zaytsev, editors, *Contemporary Mathematics: Proceedings of the 14th International Conference on Arithmetic, Geometry, Cryptography, and Coding Theory (AGCT)*, volume 637, pages 207–244. American Mathematical Society, 2015.

[9] Jordi Guàrdia, Enric Nart, and Sebastian Pauli. Single-factor lifting and factorization of polynomials over local fields. *Journal of Symbolic Computation*, 47(11):1318–1346, 2012.

[10] Enric Nart. On the equivalence of types. *Journal de Théorie des Nombres de Bordeaux, to appear*, September 2014.

[11] Kōsaku Okutsu. Construction of integral basis. I, II. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 58(1):47–49, 87–89, 1982.

[12] Jean-Pierre Serre. *Corps locaux*. Hermann, second edition, 1968.

[13] Hayden D. Stainsby. *Triangular bases of integral closures*. PhD thesis, Universitat Autònoma de Barcelona, December 2014.

Departament de Matemàtiques, Universitat Autònoma de Barcelona, Edifici C, E-08193 Bellaterra, Barcelona, Catalunya, Spain

E-mail address: hds@mat.uab.cat